(19)国家知识产权局

(12)发明专利

(10)授权公告号 CN 119156798 B
(45)授权公告日 2025.11.18

(21)申请号 202380038383.9
(22)申请日 2023.05.19
(65)同一申请的已公布的文献号
申请公布号 CN 119156798 A
(43)申请公布日 2024.12.17
(30)优先权数据
22175341.1 2022.05.25 EP
(85)PCT国际申请进入国家阶段日
2024.11.04
(86)PCT国际申请的申请数据
PCT/FI2023/050281 2023.05.19
(87)PCT国际申请的公布数据
WO2023/227828 EN 2023.11.30

(73)专利权人 古鲁洛吉克微系统公司
地址 芬兰图尔库
(72)发明人 T·卡尔凯宁
(74)专利代理机构 北京三友知识产权代理有限公司 11127
专利代理师 张亚静 赵鹏

(51)Int.Cl.
H04L 9/08(2006.01)
H04L 9/30(2006.01)
H04L 9/32(2006.01)
H04L 9/40(2006.01)
(56)对比文件
US 2019305940 A1,2019.10.03
审查员 董振兴

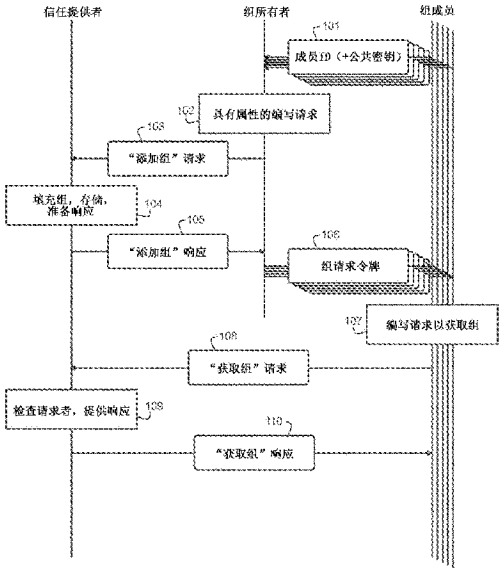
权利要求书2页 说明书13页 附图2页

(54)发明名称

用于在组之间实现安全数字通信的方法和装置

(57)摘要

一种用于建立数字密码组的装置包括密码引擎,该密码引擎被配置为从给定的输入数据产生密码产品。所述密码引擎通过产生密码产品来响应经由安全传输机构接收包含到用户标识符的请求(101)。它还通过经由所述安全传输机构发送所述密码产品(110)来响应经由所述安全传输机构接收到包含所述多个用户标识符中的一者的后续的第二请求(108)。所述密码产品是数字密码组,该数字密码组包含所述多个用户标识符,以及在由所述多个用户标识符标识的用户之间的对称密码术中使用的共用密码密钥和/或在由所述多个用户标识符标识的用户之间的通信中的非对称密码术中使用的用户特定且用户标识符相关的公共密钥。



CN 119156798 B

1.一种用于建立数字密码组的装置,所述装置包括:

密码引擎,所述密码引擎被配置为从给定的输入数据产生密码产品;以及

被联接到所述密码引擎的安全传输机构的接收端和发送端,

其中,所述密码引擎被配置为通过产生密码产品来响应经由所述安全传输机构接收到包含多个用户标识符的第一请求,

并且其中,所述密码引擎被配置为通过经由所述安全传输机构发送所述密码产品来响应经由所述安全传输机构接收到包含所述多个用户标识符中的一者的后续的第二请求,

其中,所述密码产品是包含所述多个用户标识符以及以下项中的至少一项的数字密码组:

在由所述多个用户标识符标识的用户之间的对称密码术中使用的共用密码密钥,

在由所述多个用户标识符标识的用户之间的通信中的非对称密码术中使用的用户特定且用户标识符相关的公共密钥。

2.根据权利要求1所述的装置,其中,

所述装置被配置为检查所述第一请求是否包含用于所述多个用户标识符中的每一者的相应的用户特定加密密钥,并且

所述装置被配置为通过将在所述第一请求中接收的数据扩充为包含用于所述多个用户标识符中的每一者的相应的用户特定加密密钥来响应所述第一请求不包含用于所述多个用户标识符中的每一者的相应的用户特定加密密钥的发现。

3.根据权利要求2所述的装置,其中,所述装置被配置为通过从所述装置外部的源请求和接收相应的用户特定加密密钥来执行所述扩充。

4.根据前述权利要求中任一项所述的装置,其中,所述装置被配置为对照来自另一源的对应的一条用户相关信息来检查在所述第一请求中接收的一条用户相关信息,以查找出这些条用户相关信息是否彼此匹配。

5.根据权利要求4所述的装置,其中,所述装置被配置为通过作出关于是否允许继续建立所述数字密码组的决定来响应所述这些条用户相关信息彼此不匹配的发现。

6.根据权利要求1至3中任一项所述的装置,其中,所述装置被配置为使用签名密钥来对该装置在所述密码组中包括的信息元素进行数字签名。

7.根据权利要求1至3中任一项所述的装置,其中,所述装置被配置为从所述后续的第二请求中检查该请求是去往该装置自身还是去往另一接收者,并且通过向另一接收者转发所述后续的第二请求来响应该请求是去往所述另一接收者的发现。

8.根据权利要求7所述的装置,其中,所述装置被配置为,在所述转发之前,用所述装置本身的认证替换所述后续的第二请求的原始认证。

9.一种用于建立数字密码组的方法,所述方法包括:

经由安全传输机构接收包含多个用户标识符的第一请求;

作为对接收所述第一请求的响应,产生密码产品;

经由所述安全传输机构接收包含所述多个用户标识符中的一者的后续的第二请求;以及

作为对接收所述第二请求的响应,经由所述安全传输机构发送所述密码产品,

其中,所述密码产品是包含所述多个用户标识符以及以下项中的至少一项的数字密码

组：

在由所述多个用户标识符标识的用户之间的对称密码术中使用的共用密码密钥，

在由所述多个用户标识符标识的用户之间的通信中的非对称密码术中使用的用户特定且用户标识符相关的公共密钥。

10.根据权利要求9所述的方法，所述方法包括：

检查所述第一请求是否包含用于所述多个用户标识符中的每一者的相应的用户特定加密密钥；以及

通过将所述第一请求中接收的数据扩充为包含用于所述多个用户标识符中的每一者的相应的用户特定加密密钥来响应所述第一请求不包含用于所述多个用户标识符中的每一者的相应的用户特定加密密钥的发现。

11.根据权利要求9或10所述的方法，所述方法包括：

在产生所述密码组时，使用签名密钥对包括在所述密码组中的信息元素进行数字签名。

12.根据权利要求9至10中任一项所述的方法，所述方法包括：

从所述后续的第二请求中检查该请求是去往执行所述方法的装置还是去往另一接收者；以及

通过向另一接收者转发所述后续的第二请求来响应该请求是去往所述另一接收者的发现。

13.根据权利要求12所述的方法，所述方法包括：

在所述转发之前，用执行所述方法的所述装置的认证替换所述后续的第二请求的原始认证。

14.一种包括一个或更多个机器可执行指令的一个或更多个集合的计算机程序产品，所述一个或更多个机器可执行指令被配置为在被一个或更多个处理器执行时使所述一个或更多个处理器执行根据权利要求9至13中任一项所述的方法。

用于在组之间实现安全数字通信的方法和装置

技术领域

[0001] 本发明一般涉及在由两方或更多方的组之间使用数字服务所需的安全技术领域。特别地,本发明涉及在各方之间集中建立信任的任务,所述各方此后可以依赖于在组通信或数字服务的其他种类的组相关使用中集中建立的信任。

背景技术

[0002] 数字通信中的安全性涉及多个方面,诸如机密性(只有授权方可以访问一条信息)、认证(通信方必须确信它们正在与谁通信)、完整性(一条信息没有被不允许地修改)和不可否认性(一方不能成功否认发送了某条信息)。数字通信的子属是组通信,即,数字通信和/或在预定义组的成员之间使用其他数字服务。组的成员应尽可能容易和可靠地访问组特定通信,同时确保组外的各方不能访问或以其他方式干扰通信。由于其对密码学应用的固有依赖性,这里所指的任何类型的组可以称为数字密码组。

[0003] 已知至少两种用于组通信的基本方法。在集中式解决方案中,组的成员之间的所有通信通过服务器或类似的集中式服务点来路由。在这种情况下,服务器在认证参与者和执行必要的加密和解密操作方面具有相当大的责任。另一种方法是分布式解决方案,其中通信可以直接在成员之间进行。分布式解决方案要求用户设备能够访问某些共享秘密以提供所需的安全性。

[0004] 集中式解决方案至少具有以下缺点:它们完全依赖于该组的所有活动成员对服务器的连续访问。另一方面,在分布式解决方案中,找到一种成本有效且计算合理的方式来分发共享秘密已被证明是有问题的。例如,在已知的Diffie—Hellman方法中,各方必须就提供公共密钥进行处理的顺序达成一致,以便使各方能够计算该组共有的共享秘密。而且,许多已知的分布式解决方案在各方之间建立足够信任水平的方式上是低效的,这可能使得这种解决方案易受恶意攻击。许多分布式解决方案的其他缺点与它们在使用已建立的数字密码组时对特定技术的依赖性有关。如果数字密码组与技术无关,即不依赖于与组的所有者和成员计划将来使用它的方式有关的任何特定技术,则将是更好的。

[0005] 现有技术文献US2019/0305940 A1公开了一种方法,其中,在从第二用户接收到组凭证请求时,凭证系统在通过发送组凭证来响应请求之前,使用第一用户的公共密钥检查该请求是否合法。

[0006] 另一现有技术文献US2015/0195261 A1公开了一种方法,其中,网络节点可以针对网络节点的组的成员创建和加入安全会话。

[0007] 另一现有技术文献US2010/0329463 A1公开了一种用于移动自组织网络中的组密钥管理的方法。

发明内容

[0008] 提供本发明内容以便以简化形式介绍将在以下详细描述中进一步描述的一些概念。本发明内容不旨在标识所要求保护的主题的关键特征或必要特征,也不旨在用于限制

所要求保护的主题的范围。

[0009] 目的是提供用于建立、利用和实现利用数字密码组的方法和装置，而没有上述现有技术的缺点。

[0010] 根据第一方面，提供了一种用于建立数字密码组的装置。该装置包括：密码引擎，其被配置为从给定的输入数据产生密码产品；以及联接到所述密码引擎的安全传输机构的接收端和发送端。所述密码引擎被配置为通过产生密码产品来响应经由所述安全传输机构接收到包含多个用户标识符的第一请求。所述密码引擎被配置为通过经由所述安全传输机构发送所述密码产品来响应经由所述安全传输机构接收到包含所述多个用户标识符中的一者的后续的第二请求。所述密码产品是数字密码组，该数字密码组包含所述多个用户标识符，以及在由所述多个用户标识符标识的用户之间的对称密码术中使用的共用密码密钥和/或在由所述多个用户标识符标识的用户之间的通信中的非对称密码术中使用的用户特定且用户标识符相关的公共密钥。

[0011] 根据实施方式，该装置被配置为检查所述第一请求是否包含用于所述多个用户标识符中的每一者的相应的用户特定加密密钥。然后，该装置可以被配置为通过将在所述第一请求中接收的数据扩充为包含用于所述多个用户标识符中的每一者的相应的用户特定加密密钥来响应所述第一请求不包含用于所述多个用户标识符中的每一者的相应的用户特定加密密钥的发现。这至少涉及以下优点：该装置可以灵活地适应不是所有用户特定加密密钥都被包括在第一请求中的情况。

[0012] 根据实施方式，该装置被配置为通过从该装置外部的源请求和接收相应的用户特定加密密钥来执行所述扩充。这至少涉及以下优点：该装置可以操作并灵活地适应其自身未拥有缺失的用户特定加密密钥的情况。

[0013] 根据实施方式，该装置被配置为对照来自另一个源的对应的一条用户相关信息来检查在第一请求中接收的一条用户相关信息，以查找出这些条用户相关信息是否彼此匹配。这至少涉及以下优点：可以对用户相关信息的欺骗性或以其他方式不适当的使用进行检测并做出反应。

[0014] 根据实施方式，该装置被配置为通过作出关于是否允许继续建立数字密码组的决定来响应多条用户相关信息彼此不匹配的发现。这至少涉及以下优点：所述装置的操作可以灵活地适应关于每一条信息必须有多准确的不同种类的需求。

[0015] 根据实施方式，该装置被配置为使用签名密钥来对其包括在所述密码组中的信息元素进行数字签名。这至少涉及以下优点：当稍后使用时，这样的信息元素可以携带作为信任信息的特殊价值。

[0016] 根据实施方式，该装置被配置为从所述后续的第二请求中检查该请求是去往其自身还是去往另一接收者，并且通过向所述另一接收者转发所述后续的第二请求来响应该请求是去往另一接收者的发现。这至少涉及以下优点：当在不同用户可以属于不同信任提供者的管理域的环境中操作时，可以遵循相同原理。

[0017] 根据实施方式，所述装置被配置为在所述转发之前，用所述装置本身的认证替换所述后续的第二请求的原始认证。这至少涉及以下优点：即使当进一步转发信息时，各方之间的信任关系也可以被适当地维护和使用。

[0018] 根据第二方面，提供了一种用于建立数字密码组的方法。该方法包括：经由安全传

输机构接收包含多个用户标识符的第一请求，并且作为响应，产生密码产品。该方法包括：经由所述安全传输机构接收包含所述多个用户标识符中的一者的后续的第二请求，以及经由所述安全传输机构发送所述密码产品来进行响应。所述密码产品是数字密码组，该数字密码组包含所述多个用户标识符，以及在由所述多个用户标识符标识的用户之间的对称密码术中使用的共用密码密钥和/或在由所述多个用户标识符标识的用户之间的通信中的非对称密码术中使用的用户特定且用户标识符相关的公共密钥。

[0019] 根据实施方式，该方法包括：检查所述第一请求是否包含用于所述多个用户标识符中的每一者的相应的用户特定加密密钥，以及通过将在所述第一请求中接收的数据扩充为包含用于所述多个用户标识符中的每一者的相应的用户特定加密密钥来响应所述第一请求不包含用于所述多个用户标识符中的每一者的相应的用户特定加密密钥的发现。这至少涉及以下优点：该方法灵活地适用于不是所有用户特定加密密钥都被包括在第一请求中的情况。

[0020] 根据实施方式，该方法包括：在产生所述密码组中，使用签名密钥来对包括在所述密码组中的信息元素进行数字签名。这至少涉及以下优点：该方法可以操作并灵活地适应在执行该方法的装置本身未拥有缺失的用户特定加密密钥的情况。

[0021] 根据实施方式，该方法包括从所述后续的第二请求检查该请求是去往执行该方法的装置还是去往另一接收者，以及通过向所述另一接收者转发所述后续的第二请求来响应该请求去往另一接收者的发现。这至少涉及以下优点：当在不同用户可以属于不同信任提供者的管理域的环境中操作时，可以遵循相同原理。

[0022] 根据实施方式，该方法包括：在所述转发之前，用执行该方法的装置的认证来替换所述后续的第二请求的原始认证。这至少涉及以下优点：即使当进一步转发信息时，各方之间的信任关系也可以被适当地维护和使用。

[0023] 根据第三方面，提供了一种包括一个或更多个机器可执行指令的一个或更多个集合的计算机程序产品，所述一个或更多个机器可执行指令被配置为在被一个或更多个处理器执行时使所述一个或更多个处理器执行上述类型的方法。

附图说明

[0024] 在附图中：

[0025] 图1例示了根据实施方式操作时的信息交换，以及

[0026] 图2例示了根据实施方式操作时的信息交换。

具体实施方式

[0027] 在以下描述中，参考形成本公开的一部分的附图，并且在附图中通过说明的方式示出了本公开可以被置于其中的具体方面。应理解，可以利用其他方面，并且可在不脱离本发明的范围的情况下作出结构或逻辑改变。因此，以下详细描述不应被认为是限制性的，因为本公开的范围由所附权利要求限定。

[0028] 例如，应当理解，与所描述的方法有关的公开对于被配置为执行该方法的相应设备或系统也是成立的，反之亦然。例如，如果描述了特定的方法步骤，则对应的设备可以包括用于执行所描述的方法步骤的单元，即使在附图中没有明确地描述或示出这样的单元。

另一方面,例如,如果基于功能单元来描述特定装置,则对应的方法可以包括执行所描述的功能的步骤,即使在附图中没有明确地描述或示出这样的步骤。此外,应理解,除非另外具体指出,否则本文中所描述的各种示例方面的特征可以彼此组合。

[0029] 数字密码组的一个示例是至少两个用户的组,所述至少两个用户例如(但不一定)是个人,他们希望在彼此之间安全地共享数字发送的信息,即,使得该组中的每一者都可以信任其他人是他们所声称的那个人,并且使得不是该组成员的各方不能访问共享的信息。所述用户中的一者可以充当该组的所有者或创建者。

[0030] 利用数字密码组的另一个示例是这样的一个示例,其目的是使单个用户能够安全地拥有数字属性,并在需要时呈现它以供检查。例如,负责授予驾驶执照的国家机构可以为每个有效驾驶执照持有者设置和管理这样的组。警官可以作为此类团体的成员(最好是临时成员),在这种情况下,警官将具有用于与用户的数字钱包进行安全数字通信的装置。用户驾驶特定类型车辆的权限可以作为属性存储,然后用户的数字钱包可以呈现给警察以供检查。作为另一个示例,组的所有者可以是商业企业,而成员可以是拥有忠诚卡的用户和他或她的家庭成员,在现有技术的系统中,这些家庭成员表现为与主用户相关联的从属卡的所有者。

[0031] 在本文中使用的一般定义中,数字密码组的所有者或创建者不一定是该组的成员,尽管具有作为所有者或创建者的所述角色。该情况可以用读取权限和写入权限的概念来可视化。数字密码组的成员始终具有读取权限;换句话说,只要它们仍然是成员,它们就可以连续访问为该组存储的属性。虽然所有者具有写入权限,即,有权决定将为组存储什么属性,但是在设置组之后,所有者不一定以后访问所存储的属性或成员之间的通信。然而,在许多情况下,最实际的是所有者也成为该组的成员。

[0032] 数字密码组的成员可以是用户,但至少在某些情况下也可以是组织和/或设备。在成员是用户的情况下,通常将它们称为组的成员(也称为组所有者本身),即使严格意义上,在实际数字通信中发生的各方是由所述用户和组所有者操作的电子设备。这样的电子设备可以是例如计算机、膝上型计算机、平板计算机、智能电话、便携式数字助理或包括所需处理和通信装置的一些其他电子设备。在一些情况下,用户的可编程的、可植入的电子设备可以充当这样的电子设备。

[0033] 所有对单一设备的引用都意味着还涵盖在同一用户的监督下一起工作的两个或更多个设备的组。这种两个或更多个设备的组可以被描述为由用户已经链接在一起的设备组成。采用自主权身份(Self-Sovereign Identity,SSI)的概念意味着用户已经以密码方式建立了对生成到组中的信息的控制,包括诸如管理权、处理权等权限。以密码方式建立的控制不同于仅基于绑定到特定用户ID的某些存储权限的权限:这意味着该用户拥有读取和/或写入适当信息必要的密码元素。建立密码组的目的是为组的成员提供这种拥有必要的密码元素。

[0034] 图1例示了当执行根据实施方式的方法时,信任提供者、组所有者和一个或更多个组成员之间的一些通信,以及由信任提供者、组所有者和一个或更多个组成员执行的一些操作。信任提供者也可以称为保管库,强调它代表了具有极高水平的数字安全性的机构的假定。也可用于信任提供者的类似名称是钱包提供者和缩写CA和/或VA(认证机构、验证机构)。信任提供者可以是私下操作的,或者它可以属于机构和/或在机构的监督下操作。

[0035] 为了开始设置组,组所有者应当拥有用于数字地标识要形成的组的每个成员的至少一些装置。稍后可以将更多的成员添加到组中,但是这里首先考虑为预定义数量的已知用户设置组的情况。关于稍后要添加的新成员,应当注意,将新成员添加到先前存在的组中可能意味着新成员也将获得对在添加新成员之前在组中处理的信息的访问。通过在组内单独地对先前处理过的信息进行加密,或者使用组中旧成员之间交换的密钥(例如所谓的PGP密钥,其中旧成员可能已经将他们的公共密钥分发给彼此,同时保存给自己的秘密密钥)对先前处理过的信息进行加密,可以防止新成员访问先前处理过的信息。另一种可能性是用旧成员已知的密钥对旧信息仅加密一次,并且对每个旧成员单独加密所述密钥。这最后的可能性可能是最具成本效益的可能性,因为组内共享的信息量不与成员数量成比例地增长;每个旧成员只需要安全地存储他们自己对于组内的加密信息的密钥。如果新成员绝对不需要(或不应该)访问较早处理的信息,则更直接地是可以设置新成员所属的新组。现有的组成员随后也可以从组中移除;这通常需要更新用于安全处理与组相关的信息的至少一些密钥。

[0036] 图1示意性地示出了步骤101,其中用户向组所有者传送他们希望在组中被知道的标识符。然而,应当注意,出于以下描述的目的,组所有者如何以及何时获取组成员的成员ID或其他标识符是无意义的。如果组所有者维护例如联系信息目录、人口信息的官方登记簿或客户数据库,则它可以从那里读取组成员的标识符。由于组中可能有i个成员,其中i是用作索引的正整数,所以组成员的用户标识符通常可称为UID_i。

[0037] 在步骤101(或在任何其他先前步骤),组所有者还可以从要设置的组的每个成员获取相应的公共密钥,该相应的公共密钥构成非对称密码术系统的用户特定密钥对的一半。然而,这不是必需的,因为组成员的公共密钥可能稍后才会发挥作用,如本文稍后将描述的。组中第i个成员的公共密钥可以称为PK_{UIDi}。

[0038] 在步骤102,组所有者编写添加组(AddGroup)请求,即,设置数字密码组的请求。添加组请求将被定向到信任提供者,并且它应该至少包含组成员的标识符以及打算供组成员将来使用的一个或更多个属性。作为属性的示例,这里考虑被称为P_{GO}的预共享密钥(PSK)。这种PSK可以意味着被用作组成员之间的共享秘密,例如被用作对称加密方法的加密和解密密钥。PSK和/或其他属性将作为被称为密钥库组档案的数据结构的一部分来处理,其缩写为KGA。根据正式命名,存在:

[0039] $KGA(P_{GO},\cdots)$

[0040] 其中三个句点示出KGA还可以包含其他属性,如组成员的标识符UID_i和/或(至少一些)组成员的公共密钥PK_{UIDi}。如果要明确列出这些,则正式命名可以是:

[0041] $KGA(P_{GO},UID_i,PK_{UIDi},\cdots)$。

[0042] KGA中可能的其他属性的示例包括但不限于:数字密码组的名称和/或其他标识符,示出例如创建和修改数字密码组的时间的时间戳,示出数字密码组应保持有效多长时间的到期数据,请求将被定向到的信任提供者的标识符,以及与数字密码组的任何方面有关的元数据。

[0043] 为了安全起见,步骤102应当包括加密KGA。生成加密密钥K_{KGA}的有利方式是:

[0044] $K_{KGA}=SHA2(X25519(SK_{UID},PK_{VID})||PK_{VID}||PK_{UID}||n)$

[0045] 其中,SHA2()表示对圆括号中的参数执行安全散列算法2,X25519()表示对圆括

号中的参数应用Curve25519椭圆曲线Diffie—Hellman方法。字母n表示密码随机数,例如12位的唯一随机数。双竖直线||表示逐位逻辑OR运算。密钥PK_{VID}和PK_{UID}分别是信任提供者(PK_{VID})和组所有者(PK_{UID})的公共密钥。

[0046] KGA的加密可以例如使用AES256—GCM方法来执行,这意味着伽罗瓦(Galois)/计数器模式下的256位AES。使用到目前为止引入的符号,加密的KGA可以表示为:

[0047] $Enc(K_{KGA},KGA(P_{G0},UID_i,PK_{UIDi},\cdots))$

[0048] $=AES256\text{-}GCM(SHA2(X25519(SK_{UID},PK_{VID})$

[0049] $||PK_{VID}||PK_{UID}||n),m,n,KGA(P_{G0},UID_i,PK_{UIDi},\cdots))$

[0050] 其中,字母m表示用于加密认证标签的MAC或消息认证码。

[0051] 此外,有利的是使步骤102包括生成非对称密码术方法的一对临时密钥。这些临时密钥在这里被称为PK_{GRT}和SK_{GRT},其中PK表示公共密钥,SK表示秘密密钥,下标GRT来自词语组请求令牌(Group Request Token)。组所有者将保持秘密密钥SK_{GRT}被存储,并在添加组请求中向信任提供者提供公共密钥PK_{GRT}。这样,信任提供者可以使用公共密钥PK_{GRT}来加密其最终响应,从而确保只有组所有者能够解密它。这些密钥的短暂性质不是强制性的,但是它增加了安全性,因为后来会持有这些密钥中的任一者的恶意方将很少使用它。

[0052] 将完成的添加组请求从组所有者发送到信任提供者,如图1中的步骤103所示。图1中的命名添加组和所有其他特定命名仅是示例性的,不应理解为在任何意义上的限制;自然地,一些其他命名可以用于该消息。也不必在单个消息中传送这里描述的所有信息,而是可以使用通过公共通信信道或甚至多个信道的多个传输。使用上面介绍的符号,步骤103的添加组请求可以至少包含临时公共密钥PK_{GRT}和加密的KGA。

[0053] 在步骤103,最有利地是使用安全传输机构将添加组请求从组所有者传送到信任提供者。这种安全传输机构的非限制性示例是其中可以使用TLS(传输层安全)协议的数字通信信道。这里被称为信任提供者的装置包括这种安全传输机构的接收端和发送端,该安全传输机构联接到能够执行密码操作的密码引擎。经由安全传输机构的接收和发送不一定通过相同或相似的信道或连接,尽管也不排除这种情况。

[0054] 图1中的步骤104通常可以表征为信任提供者设置所请求的数字密码组并将其以数据结构的形式存储,所述数据结构稍后可以在请求时传送到组的成员。步骤104的特征还在于,信任提供者的装置中的密码引擎通过产生密码产品来响应经由所述安全传输机构接收到包含多个用户标识符(UID_i)的第一请求(即,添加组请求103)。这里,词语密码产品指的是数字密码组,该数字密码组至少包含组成员的用户标识符以及用于实现组成员之间的安全通信的一个或更多个密钥。数字密码组还可包含各种其他信息,如本文稍后将更详细地描述。

[0055] 当KGA以加密形式出现在添加组请求103中时,信任提供者的装置应该首先解密它。假定组所有者使用上述用于生成加密密钥的方法来加密添加组请求103中的KGA,则信任提供者的装置可以将密钥重新生成为

[0056] $K_{KGA}=SHA2(X25519(SK_{VID},PK_{UID})||PK_{VID}||PK_{UID}||n)$

[0057] 并且使用所重新生成的密钥来解密KGA。

[0058] 上面已经指出,当构造添加组请求103时,组所有者不必拥有所有(或甚至任何)组成员的用户特定(公共)加密密钥。为此,有利的是,作为步骤104的一部分,配置信任提供者

的装置以检查所接收的添加组请求103是否包含用于每个用户标识符的相应的用户特定加密密钥。如果不是,则信任提供者的装置可以被配置为将在所述第一请求中接收的数据扩充为包含用于所述多个用户标识符中的每一者的相应的用户特定加密密钥。

[0059] 一种可能性是信任提供者已经知道相应的用户特定(公共)加密密钥,例如基于它与所述用户的一些先前通信。作为另一种可能性,信任提供者的装置可以被配置为通过从装置外部的源请求和接收相应的用户特定加密密钥来执行所述扩充。作为示例,可以考虑存在彼此链接的两个或更多个信任提供者的情况。每个这样的信任提供者具有其先前已知的用户数据库:信任提供者例如可以是某些用户之前已经与之通信的不同机构,和/或各自具有其自己的客户数据库的不同商业企业。用户特定加密密钥(特别是公共密钥)可以常规地存储在这样的数据库中,每个这样存储的加密密钥与在添加组请求中使用的类似类型的相应用户标识符具有明确的关系。信任提供者的装置可以向一个或更多个这样链接的信任提供者发送请求,并作为响应获取所请求的用户特定加密密钥。

[0060] 类似的原则也适用于要被包括在密码组中的其他数据:信任提供者的装置可以通过生成任何缺失的信息元素(或者通过其自己、或者通过从链接的其他源请求、或者通过两者)来扩充密码组的内容。如果需要,信任提供者的装置根据管理密码组的创建和处理的预定义规范来执行任何这种扩充。

[0061] 信任提供者的装置可以被配置为对照来自另一个源的对应的一条(用户相关)信息来检查在添加组请求103中接收的任何一条信息(例如,用户相关信息)。如果被执行,则这种检查的目的是要查找出这些条用户相关信息是否彼此匹配。例如,如果添加组请求103包含一个或更多个用户特定(公共)加密密钥,则信任提供者的装置可以将这些与它自己的数据库进行比较,或者如果在它自己的数据库中没有查找到,则它可以再次向可能链接的其他信任提供者进行请求,就像上述请求用户特定加密密钥的情况。

[0062] 每个用户(或符合组中成员资格的其他方)可以被假定为“属于”某个信任提供者,或者最初由某个信任提供者安全地标识。其装置接收添加组请求103的信任提供者可以不是最初安全地标识所有将被包括为新组成员的那些用户的信任提供者。换句话说,添加组请求103可以包含组的一个或更多个预期成员的UID,该一个或更多个预期成员“属于”一个或更多个不同信任提供者,而不是其装置接收到添加组请求的信任提供者。在这种情况下,一种可能性是信任提供者的装置简单地留下空的空间,如果它“自己的”用户中的一者有问题,则它将在该空间中使用用户特定加密密钥。这种操作方式,即让“外来”用户的用户特定加密密钥为空,可能会产生本文稍后描述的某些进一步后果。

[0063] 如果所述多条用户相关信息彼此不匹配,则信任提供者的装置可以作出关于是否允许继续建立数字密钥组的决定。肯定的和否定的决定都是可能的,这取决于信任提供者的装置已经被编程为如何操作以及它应用了何种决策标准。

[0064] 上面已经指出,除了用户标识符之外,数字密码组在完成时应当包含一个或更多个密钥,以实现组成员之间的安全通信。用户特定(公共)加密密钥可以满足这个要求,因为可以假定每个用户具有安全存储的对应的秘密密钥。这种密钥的另一个示例是上述称为P_{GO}的预共享密钥(PSK),P_{GO}通常定义为在由用户标识符标识的用户之间的对称加密中使用的公共加密密钥。如果组所有者已经生成P_{GO},则信任提供者的装置可以简单地从解密的KGA读取它,并将其存储为数字密码组的一部分。作为另一另选方案,信任提供者的装置可以生成

这样的PSK,并将其存储为数字密码组的一部分。

[0065] P_{GO}或其他PSK是被包括在密码组中的属性(或信息元素)的示例,组成员随后必须能够完全依赖它。为了提供这种安全性,有利的是由组所有者(如果组所有者已经生成P_{GO})和/或由信任提供者的装置对P_{GO}或其他PSK进行数字签名。根据已知原理,签名方使用其秘密签名密钥进行数字签名,使得其他方稍后可以使用签名方的对应的公共验证密钥来验证所讨论的信息元素的完整性。

[0066] 为了在该方法的后续阶段中提供附加的安全性,有利的是,作为步骤104的一部分,配置信任提供者的装置以生成非对称密码术方法的另一对临时密钥。这对临时密钥在这里将被称为下标GAT,表示组访问令牌。作为非限制性示例,信任提供者的装置可以生成秘密GAT密钥SK_{GAT}为:

[0067] $SK_{GAT}=RNG(256)$

[0068] 其中,运算符RNG()表示生成具有与括号中的(十进制)数一样多位的随机二进制数。然后,对应的公共密钥PK_{GAT}可以例如作为来自$scalarbasemult(SK_{GAT})$的公共密钥来生成。这里,scalarbasemult()是基于椭圆曲线(例如Curve25519)的函数,当给定秘密密钥作为输入时,该函数确定性地返回对应的公共密钥。函数的名称可能会取决于所使用的源而改变,但在撰写本文时,可在https://doc.libsodium.org/找到关于原始scalarmult()函数的文档。每当需要生成一对秘密密钥和公共密钥时,这也可以使用给出两个密钥作为输出的适当的单个函数来完成。

[0069] 信任提供者的装置可以被配置为根据在步骤104在向组所有者发送响应之前创建该数字密码组的情况(或者是在与任何其他组成员通信之前更新先前创建的数字密码组的情况)还是加密是否是与除组所有者之外的组成员通信相关联地完成的情况而以稍微不同的方式加密所创建或更新的KGA,参见图1中的步骤109。在第一种情况下,有利的可能性是利用先前获得的特定于组所有者的密钥。在共同未决的专利申请号EP22157019.5中描述了创建和处理这样的密钥的有利方法,该专利申请在本文申请日尚未公开。所讨论的密钥在所述方法中称为SK_{UAT},其中下标UAT来自用户访问令牌。对新创建的KGA进行加密的处理可以涉及生成共享秘密SS_{GAK}为:

[0070] $SS_{GAK}=scalarmult(SK_{GAT},PK_{GRT})$

[0071] 其中,下标GAK来自组存档密钥。函数scalarmult()是基于椭圆曲线(例如Curve25519)的函数,其返回双方之间的计算共享秘密,使得在依赖以数学方式链接的密钥对建立的安全性的同时,无需发送实际密钥。然后,新创建的KGA可以被加密为:

[0072] $Enc(SS_{GAK},KGA(\cdots))$

[0073] 其中,三个句点通常再次表示包括在KGA中的所有信息。然而,如果情况是更新先前用SS_{GAK}作为密钥加密的KGA中的一者,则在与除组所有者之外的任何组成员通信之前,更新操作可被描述为:

[0074] $Update(Dec(SS_{GAK},KGA(\cdots)))$

[0075] 此后,可以与上述类似地进行新的加密。

[0076] 如果加密是作为步骤109的一部分来完成的,则与除组所有者之外的组成员的通信相关联,可以通过利用本文前面介绍的秘密GAT密钥SK_{GAT}来获得额外的安全性。

[0077] 在这种情况下,共享秘密SS_{GAK}可以被获得为:

[0078] SS_{GAK}=scalarmult(SK_{GAT},PK_{GRT})

[0079] 其中,下标GAK来自组存档密钥。然后,可以将KGA加密为

[0080] Enc(SS_{GAK},KGA(…))

[0081] 这样,以用SS_{GAK}加密的形式将KGA存储在信任提供者的装置中,其目的是始终需要来自信任提供者外部的源的密钥来解密所存储的KGA。因此,即使在信任提供者处的安全性被损害并且所存储的KGA被暴露,它们对攻击者几乎没有用处,因为即使信任提供者也不能在没有那些必须来自组所有者或其他组成员中的一者的密钥组件的情况下访问它们的加密内容。

[0082] 作为上述过程步骤的结果,KGA(即在步骤104产生的信任提供者的装置的密码引擎的密码产品)可以被描述为例如:

[0083] KGA(P_{GO},UID_i,PK_{UIDi},PID,GID,GMD,…)

[0084] 其中,P_{GO}是组的PSK,UID_i标记由其标识符列出的组成员(包括组所有者),PK_{UIDi}标记组成员的(公共)用户特定加密密钥,PID或提供者ID是信任提供者的公共标识符,GID或组ID是组的公共标识符,以及GMD或组元数据标记与组相关联的所有可能的元数据。组所有者的标识符和/或公共密钥可以被挑选出来以允许将它或它们与UID_i和PK_{UIDi}的其余部分区分开。

[0085] 为了增强密码组中属性的可信性,有利的是将信任提供者的装置配置为使用其拥有的签名密钥对其在密码组中包括的信息元素进行数字签名。这使得组的所有成员稍后能够确保从密码组读取的属性是正确的,即它们的原创性和完整性未被损害。

[0086] 信任提供者的装置将添加组响应发送到组所有者的步骤如图1中的步骤105所示。与较早在步骤103的添加组传输类似,信任提供者的装置有利地在将KGA发送到添加组响应105中的组所有者之前加密KGA。这种加密的有利形式是:

[0087] Enc(K_{KGA},KGA(…))

[0088] =AES256-GCM(SHA2(X25519(SK_{VID},PK_{UID})

[0089] ||PK_{VID}||PK_{UID}||n),m,n,KGA(…))

[0090] 在步骤105之后,组所有者具有关于组的所有必要信息,包括在步骤104期间信任提供者提供其自己的动作和/或从链接的其他信任提供者或其他源请求的扩充信息。另外,组所有者知道关于组的所有必要信息被安全地存储在信任提供者的装置中,并且准备从那里分发到组的成员。

[0091] 步骤106表示组所有者指示组成员联系信任提供者并从信任提供者的装置下载KGA。使组成员能够这样做的一个有利方式是向他们发送组请求令牌的副本,即,临时公共密钥PK_{GRT}。附加地或另选地,在步骤106,组所有者可以向组成员发送关于组的其他信息。

[0092] 图1中所示的其余步骤仅关于一个组成员示出,以便保持图形清晰。应当对所有组成员执行类似的步骤以使该组完全可操作。然而,即使一个或更多个组成员未能完成其部分,已经完成对应步骤的执行的那些组成员也可能已经利用该组。这里可以注意到,通过使用信任提供者作为与组相关的信息元素的安全存储部可以获得某些优点,即使组中仅一个成员实际上将执行这些步骤并在将来使用密码组。

[0093] 步骤107表示组成员编写用于获取关于组的必要信息的请求,并且步骤108表示组成员将所述请求(此处称为获取组(GetGroup)请求)发送到信任提供者。步骤108的发送与

较早的步骤103的发送是类似的,因为它可以利用安全传输机构,如其中可以使用TLS(传输层安全)协议的数字通信信道。

[0094] 获取组请求108应当允许信任提供者确保发送者(即,组成员)是被允许接收作为组成员操作所需的KGA的那些发送者中的一者。有利地,获取组请求108因此至少包含用户标识符UID,然后信任提供者可以将用户标识符UID与先前从组所有者接收的用户标识符UID_i的列表进行比较。使获取组请求108包含用户标识符UID的一种有利方式是使其包含请求方的证书,该证书包含UID和请求方的公共密钥两者。在这种情况下,信任提供者可以使用UID用于上述目的,并使用公钥来保护KGA,该KGA将作为响应发送给请求方。

[0095] 另外,获取组请求108有利地包含组请求令牌,即,临时公共密钥PK_{GRT}。获取组请求可以包含的其他可能的信息元素(至少在请求组成员先前从组所有者获得它们的情况下)包括但不限于组标识符GID、对组所有者的标识符的引用,各种类型的已签名或未签名属性,和/或与组相关的任何元数据。

[0096] 图1中的步骤109通常表示信任提供者的装置被配置为响应于接收到获取组请求108而进行的所有检查。基本上,信任提供者的装置中的密码引擎被配置为通过经由安全传输机构发送先前产生的密码产品(即,数字密码组)来响应经由所述安全传输机构接收到获取组请求108(其包含先前在添加组请求103中接收的多个用户标识符中的一者)。

[0097] 考虑到KGA先前以加密形式存储在信任提供者的装置中,该装置可以首先重新生成解密所需的密钥SS_{GAK}为

[0098] $SS_{GAK}=scalarmult(SK_{GAT},PK_{GRT})$

[0099] 并且然后执行解密

[0100] $Dec(SS_{GAK},KGA(\cdots))$。

[0101] 然后,该装置可以通过以下操作继续再次加密KGA(这次用于发送到请求组成员),即,通过提供

[0102] $n=RNG(96)$

[0103] 作为随机数,并且提供

[0104] $K_{KGA}=SHA2(X25519(SK_{VID},PK_{UID})||PK_{VID}||PK_{UID}||n)$

[0105] 作为加密密钥(使用该特定用户的PK_{UID},如果在获取组请求中接收到证书则从证书中读取),然后再加密:

[0106] $Enc(K_{KGA},KGA(\cdots))$

[0107] $=AES256\text{-}GCM(SHA2(X25519(SK_{VID},PK_{UID})$

[0108] $||PK_{VID}||PK_{UID}||n),m,n,KGA(\cdots))$。

[0109] 从安全性的观点来看,特别有利的是要求上述证书始终来自请求者,因为在步骤109(以及稍后在图2中的步骤210),密钥库组档案对于用户来说相对于特定用户的公共密钥PKUID是安全的。证书可以出现在如上所述的获取组请求中,但是它也可以通过一些其他基于PKI的解决方案来使信任提供者的装置获知,例如根据同一申请人的共同未决欧洲专利申请EP22157019.5中描述的方法。附加地或另选地,如果存在适当的智能身份证、护照或对应的文档,则信任提供者的装置可以根据规范X.509从其读取证书作为RSA或ECC证书。

[0110] 类似地,从安全性的观点来看,非常有利的是要求由信任提供者的装置来对证书进行签名,或者在若干相互链接的信任提供者的情况下,由这种相互链接的信任提供者中

的一者的装置来对证书进行签名。然后接收证书的任一方可以检查证书的完整性和真实性,并确定它是由可信方(即,由信任提供者或相互链接的信任提供者中的一者)签名的。这反过来证明包含在证书中的公共密钥可以是可靠的。

[0111] 在随机数n中,可以注意到它与IETF接受的AES—256GCM算法的要求有关。它向加密密钥提供32个附加位的增强的安全性,特别是当它被使用更长的时间时,直到最大350GB。

[0112] 图1中的步骤110表示信任提供者的装置向请求加密的KGA的组成员发送加密的KGA。该发送在图1中被标记为获取组响应,以强调其与先前获取组请求108的关联。类似于较早的命名添加组,命名获取组自然也仅是一个示例,并且也可以使用其他命名。

[0113] 作为应用图1中所示类型的方法的示例,可以考虑这样的情况,其中例行巡逻的警官使公民停止,并且想要检查公民驾驶该特定类型的车辆的权限。负责授予驾驶执照的国家机构可以充当组所有者。先前,在授予当前有效的驾驶执照时,机构可能已经形成了数字密码组,其中它本身是组所有者,并且公民是成员。在形成该组时,机构可以将允许的车辆类型作为属性传送给信任提供者,并要求信任提供者对这些属性进行数字签名。当公民随后通过发送对应的获取组请求加入该组时,数字签名的属性被存储在“数字钱包”中,即在公民的用户设备中的专用存储位置。属性可以与基本文档(在该示例中:驾驶执照)一样长时间地保持有效。

[0114] 在从公民获知(公共)用户标识符之后,警官可以向机构发送请求,给出他们自己的用户ID(以及可能的公共密钥),并且还将公民的用户标识符作为属性添加到请求中。然后,机构可以向信任提供者发送添加组请求,实质上是请求警官临时添加到先前形成的数字密码组,该数字密码组具有从公民接收属性“允许的车辆类型”的权限。作为另选方案,警官(或作为机构的警察部队,当个别警官在值班时具有对应的衍生权限)可以早已成为该组的(永久的或至少长期的)成员,以便允许离线检查公民的驾驶执照。

[0115] 信任提供者的装置可以执行所请求的对数字密码组的添加。包含组请求令牌的指示随后将到达警官的用户设备。然后当警官的用户设备向信任提供者发送获取组请求时,它最终接收包含它需要的信息的获取组响应。在这一轮通信期间,一个或更多个属性可能已被添加到数字密码组:例如,时间限制有效性信息仅允许警官的用户设备在短时间内保持组成员。

[0116] 一旦警官成为数字密码组的成员,公民和警官的用户设备可以进入本地通信,其中公民的用户设备向警官的用户设备呈现先前获得的、被数字签名的属性“允许的车辆类型”。由于数字签名,后者能够验证所呈现的属性是有效的。当完成所有检查时,警官的用户设备可以经由与添加它时类似的一轮通信从数字密码组中移除,或者可以简单地依赖于先前提到的时间信息来允许警官在数字密码组中的成员资格到期。作为另一另选方案,在组中存在警察的永久或至少长期的成员资格。

[0117] 在如上所述的示例情况下,机构可能希望定期更新密码组的属性,以便确保没有过时的属性(或至少没有严重过时的属性)保持存储在用户的设备中。公民的用户设备可以遵循已知的更新时间表和/或当机构提示这样做时,从信任提供者获取更新的密码组。

[0118] 图2例示了当执行根据实施方式的方法时,两个信任提供者、组所有者和组成员之间的一些通信以及由这两个信任提供者、组所有者和组成员执行的一些操作。作为本实施

方式的背景,可以回忆每个用户可以“属于”其选择的信任提供者的假定。在这个示例中,中间的两条竖直线表示信任提供者的装置,而右边和左边的两条竖直线相应地表示组所有者和组成员。出于说明的目的,图2中所示的示例可以被认为涉及组所有者想要与组成员设置受保护的电话呼叫的实际使用情况。

[0119] 图2中的步骤201与图1中的步骤101类似,组所有者应当以某种方式或另一种方式获取组成员的标识符。这个步骤甚至可能早就发生了,例如,典型的是用户将彼此的电话号码存储在其用户设备中。

[0120] 步骤202也可与图1中的对应步骤102类似,它表示组所有者的用户设备执行旨在设置受保护呼叫的步骤,即创建其中可发生受保护呼叫的密码组。所编写的请求被示为步骤203,并被命名为添加组请求,非常类似于图1的步骤103。组所有者将添加组请求203发送到其“自己的”信任提供者。最有利地,添加组请求203包含加密的KGA(密钥库组档案)和组请求令牌PK_{GRT},其中KGA包含预共享密钥(本文前面称为PSK或P_{GO})和应当对其进行受保护呼叫的组成员的标识符UID(以及可能的公共密钥PK_{UID})。

[0121] 图4中的步骤204可与图1中的步骤104类似,它表示信任提供者(组所有者“属于”的那一个信任提供者)设置所请求的密码组并以数据结构的形式存储它,该数据结构稍后可在请求时被传送给组成员。该信任提供者的装置中的密码引擎通过产生密码产品(即,通过创建所请求的密码组)来响应经由安全传输机构接收到包含多个用户标识符(组所有者和组成员的UID)的添加组请求203。步骤205是信任提供者的装置发送回组所有者的添加组响应,再次与图5中的步骤105非常类似。

[0122] 在步骤206,组所有者的用户设备向组成员的用户设备至少发送组请求令牌PK_{GRT}和组所有者的信任提供者的标识符VID。尽管在图2中未明确地显示为单独的步骤,但组成员的用户装置使用此信息来编写用于获得密码组(的加密的KGA)的请求。然而,由于组成员属于与组所有者不同的信任提供者,所以步骤207的获取组请求不被发送到当前保存密码组的存储数据的信任提供者。相反,组成员的用户设备将获取组请求207发送到其自己的信任提供者。

[0123] 用户与他们的信任提供者之间的预先存在的关系意味着,他们对应的设备和装置特别容易和直接地设置和利用用于发送图2所示的请求和响应的安全传输机构。在某些先前阶段,在每个用户与他们响应的信任提供者之间可能已经交换了足够的密钥和/或其他共享秘密信息,以便在需要时既快速又安全地设置这些通信连接。这同样适用于信任提供者之间的通信。这样,依赖这里所指的共享秘密对于用于建立它们的技术是不可知的。与PKI(公共密钥基础结构)一样,使用何种加密(ECC、RSA或其他)和算法并不重要。合理的是假定例如机构可能经常依赖于比最先进的个人用户和私人企业更旧的加密技术,因此在最有利的情况下,系统和方法应该允许用任何种类的PK密钥进行操作。

[0124] 上述对共享秘密的引用可以有利地表示数学上链接的密钥对之间的计算秘密,其来自根据例如ECC或RSA算法的一者自身的秘密密钥(SK)和另一个者的公共密钥(PK)的乘积。

[0125] 在步骤208,组成员的信任提供者接收获取组请求207,并注意到它除了组请求令牌之外还包含外部VID。换句话说,获取组请求207中的VID不是组成员的信任提供者的VID,而是标识组所有者的信任提供者。基于信任提供者之间先前建立的链接关系,组成员的信

任提供者能够将获取组请求转发到组所有者的信任提供者，如图2中的步骤209所示。然而，组成员的信任提供者使用其自身的凭证(而不是组成员的凭证)来认证它转发到组所有者的信任提供者的获取组请求209。

[0126] 图2中的步骤210与图1中的步骤109类似，组所有者的信任提供者的装置中的密码引擎响应经由安全传输机构(用于在信任提供者之间通信)接收到获取组请求209。所述请求包含先前在添加组请求203中接收的多个用户标识符中的一者(组成员的标识符)。组所有者的信任提供者的装置通过经由安全传输机构向组成员的信任提供者发送先前产生的密码产品(即，数字密码组)来响应(参见图2中的步骤211)。

[0127] 组成员的信任提供者不需要知道其接收的获取组响应211中的任何内容。相反，将在两个信任提供者之间使用的认证机制替换为在组成员的信任提供者与组成员之间使用的认证机制就足够了。相应转发的获取组响应如图2中的步骤212所示。在接收到它并对其内容进行解密之后，组成员的用户设备准备好与组所有者的用户设备进行安全通信，如图2的步骤213所示。

[0128] 与上述方法和装置相关联的显著优点中的一者是可以应用通常称为DID的分散标识符的实践。为了建立用于数字通信的信任关系，信任提供者可以出于不同目的而具有用户的不同(公共)密码密钥和签入信息。其一个有利结果是可以在不同级别上应用控制。另一个是组成员匿名和/或假名出现的可能性。根据使用情况，组的成员可能甚至彼此看起来匿名或作为假名操作，但完全依赖于信任提供者保证的信任关系。同样可能的是，该组的成员可以彼此标识，而它们保持对非成员是不可标识的。

[0129] 本文给出的任何范围或设备值可以被扩展或更改而不失去所寻求的效果。除非明确地禁止，否则任何实施方式都可以与另一实施方式组合。

[0130] 虽然已经用结构特征和/或动作专用的语言描述了本主题，但是应当理解，所附权利要求中定义的主题不必限于上述具体特征或动作。相反，上述具体特征和动作是作为实现权利要求的示例而公开的，并且其他等效特征和动作旨在处于权利要求的范围内。

[0131] 应当理解，上述益处和优点可涉及一个实施方式或可涉及若干实施方式。实施方式不限于解决任何或所有所述问题的实施方式或具有任何或所有所述益处和优点的实施方式。还将理解，对“一个”项的引用可以指这些项中的一个或更多个。

[0132] 本文所述的方法的步骤可以以任何合适的顺序进行，或在适当的情况下同时进行。另外，在不脱离本文所述主题的精神和范围的情况下，可以从任何方法中删除各个框。以上描述的任何实施方式的方面可以与所描述的任何其他实施方式的方面组合以形成进一步的实施方式，而不损失所寻求的效果。

[0133] 术语“包括”在此用于表示包括所标识的方法、框或元素，但是这样的框或元素不包括排他性列表，并且方法或装置可以包含附加的框或元素。

[0134] 应当理解的是，以上描述仅仅是作为示例给出的，并且本领域技术人员可以进行各种修改。以上说明书、示例和数据提供了对示例性实施方式的结构和使用的完整描述。尽管上文已经以一定程度的特殊性或参考一个或更多个单独的实施方式描述了各种实施方式，但是本领域技术人员可以在不脱离本说明书的精神或范围的情况下对所公开的实施方式进行多种改变。

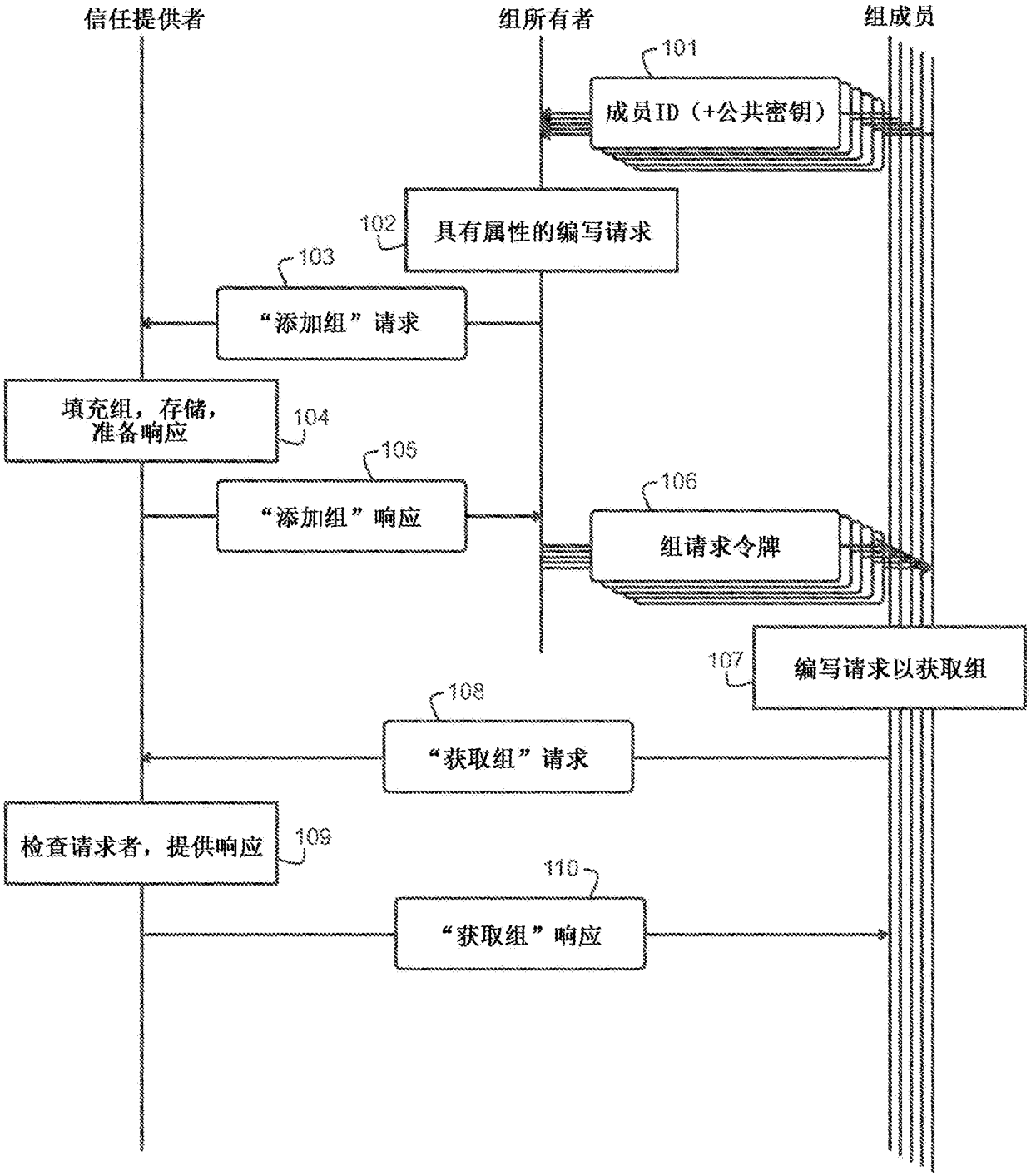

信任提供者
组所有者
组成员
101
成员ID（+公共密钥）
102
具有属性的编写请求
103
“添加组”请求
填充组，存储，
准备响应
104
105
“添加组”响应
106
组请求令牌
107
编写请求以获取组
108
“获取组”请求
检查请求者，提供响应
109
110
“获取组”响应

图1

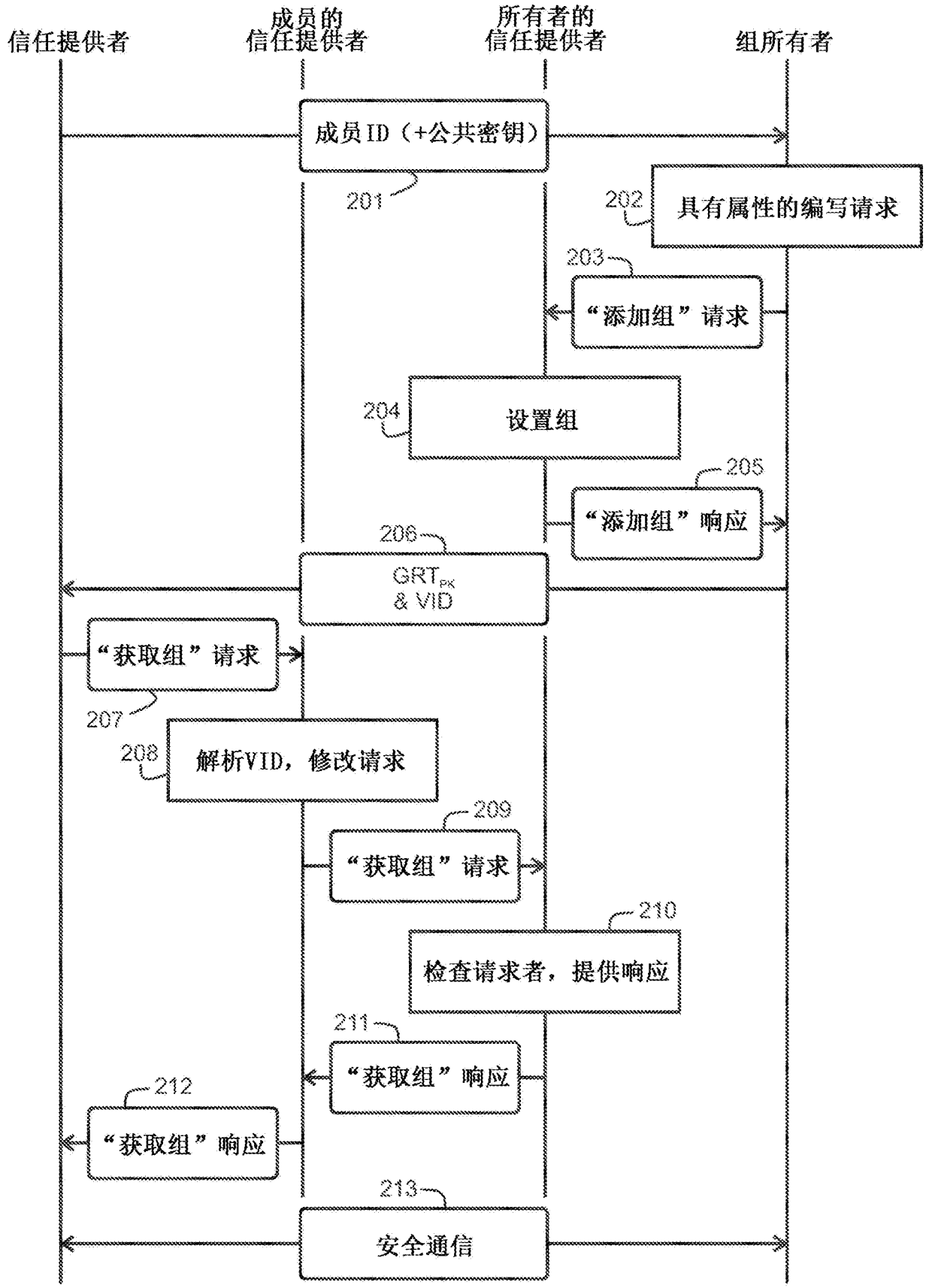

信任提供者
成员的信任提供者
所有者的信任提供者
组所有者
成员ID（+公共密钥）
201
202
具有属性的编写请求
203
“添加组”请求
204
设置组
205
“添加组”响应
206
GRT$_{PK}$ & VID
“获取组”请求
207
208
解析VID，修改请求
209
“获取组”请求
210
检查请求者，提供响应
211
“获取组”响应
212
“获取组”响应
213
安全通信

图2