(19)国家知识产权局

(12)发明专利

(10)授权公告号 CN 111030813 B
(45)授权公告日 2024.06.11

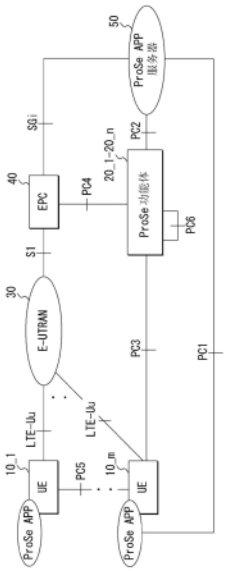
(21)申请号 201911356997.3
(22)申请日 2014.08.27
(65)同一申请的已公布的文献号
申请公布号 CN 111030813 A
(43)申请公布日 2020.04.17
(30)优先权数据
2013-225200 2013.10.30 JP
2013-226681 2013.10.31 JP
(62)分案原申请数据
201480060054.5 2014.08.27
(73)专利权人 日本电气株式会社
地址 日本东京都
(72)发明人 张晓维
阿南德·罗迦沃·普拉萨德
(74)专利代理机构 北京林达刘知识产权代理事务所(普通合伙) 11277
专利代理师 刘新宇
(51)Int.Cl.
H04L 9/08(2006.01)
H04W 4/02(2018.01)
H04W 8/00(2009.01)
H04W 8/08(2009.01)
H04W 12/041(2021.01)
H04W 12/0431(2021.01)
H04W 12/08(2021.01)
(56)对比文件
"S3-130794".《3GPP tsg_sa\WG3_Security》.2013,第6.X.2-6.X.4节.
"S3-130882_cl".《3GPP tsg_sa\WG3_Security》.2013,第6.3.2-6.3.4节.
审查员 代悦宁
权利要求书1页 说明书17页 附图13页

(54)发明名称

用户设备及其方法

(57)摘要

本发明涉及移动通信系统、网络节点、用户设备及其方法。为了有效地确保ProSe中的直接通信的安全,ProSe功能体(20)从第三方获取各UE(10_1～10_m)的根密钥以得出用于与不同UE安全地进行直接通信的一对会话密钥,并且将所获取的根密钥分发给各UE(10_1～10_m)。各UE(10_1～10_m)通过使用分发的根密钥其中之一来得出会话密钥。此外,构成通信系统且在UE彼此邻近的情况下允许彼此进行直接通信的多个UE在成功地向支持直接通信的节点登记了这些UE时,经由该节点在这些UE之间共享这些UE的公钥。各UE通过使用公钥其中之一来至少验证针对直接通信的请求。



CN 111030813 B

1.一种用于基于邻近的服务即ProSe的移动通信系统中的UE即用户设备,所述UE包括:

用于连接到第一网络节点的部件;

用于通过使用第三网络节点从所述第一网络节点接收根密钥和用于识别所述根密钥的标识符的部件;

用于基于所述根密钥得出会话密钥的部件;以及

用于在所述UE与另一UE之间进行直接通信的部件,

其中,所述直接通信通过所述会话密钥来保护,以及

所述另一UE向第二网络节点进行登记并且基于由从所述第二网络节点接收到的标识符所识别的所述根密钥得出所述会话密钥。

2.一种用于基于邻近的服务即ProSe的移动通信系统中的UE即用户设备的方法,所述方法包括:

向第一网络节点登记;

通过使用第三网络节点从所述第一网络节点接收根密钥和用于识别所述根密钥的标识符;

基于所述根密钥得出会话密钥;以及

在所述UE与另一UE之间进行直接通信,

其中,所述直接通信通过所述会话密钥来保护,以及

所述另一UE向第二网络节点进行登记并且基于由从所述第二网络节点接收到的标识符所识别的所述根密钥得出所述会话密钥。

用户设备及其方法

[0001] 本申请是申请日为2014年08月27日,申请号为201480060054.5、题为“基于邻近的服务中的安全直接通信所用的设备、系统和方法”的发明专利申请的分案申请。

技术领域

[0002] 本发明涉及ProSe(Proximity based Service,基于邻近的服务)所用的设备、系统和方法。特别地,本发明涉及ProSe中的直接通信的安全,并且考虑到网络授权的直接通信。此外,本发明涉及使用PKI(Public-Key Infrastructure,公钥基础设施),并且不仅考虑到一对一直接通信,而且还考虑到一对多直接通信。

背景技术

[0003] 3GPP(第三代合作伙伴计划)已经研究了直接通信(Direct Communication)(参见非专利文献1和2)。

[0004] 针对直接通信的关键问题是确保接口PC5的安全。如何利用最少的信令确保接口PC5的安全以及如何利用最少的信令从信任源建立安全上下文(例如包括密钥得出、分配、更新)是重要的事情。

[0005] 注意,接口PC5是UE(多于一台的用户设备)之间的参考点,使得UE可以经由该接口PC5进行直接通信。针对ProSe发现、直接通信和UE中继的控制面和用户面,使用接口PC5。UE直接通信可以直接执行或者经由LTE-Uu执行。

[0006] 现有技术文献

[0007] 非专利文献

[0008] 非专利文献1:3GPP TR 33.cde,"Study on security issues to support Proximity Services(版本12)",V0.2.0,2013-07,第5.4、5.5和6.3条,第11、12和13-20页

[0009] 非专利文献2:3GPP TR 23.703,"Study on architecture enhancements to support Proximity Services(ProSe)(版本12)",V0.4.1,2013-06,第5.4、5.12和6.2条,第13、17、18和62-82页

发明内容

[0010] 发明要解决的问题

[0011] 然而,本申请的发明人发现3GPP SA3(安全工作组)的当前解决方案存在以下缺陷。

[0012] 1)对MME(移动管理实体)的影响:该解决方案需要在包括密钥材料(key material)分配的直接通信过程中涉及MME。

[0013] 2)每当UE想要与其它UE进行直接通信时发生密钥分配过程,这不仅产生信令而且还是在出现并行的一对一通信的情况下发生的。因此,该解决方案不够有效。

[0014] 因此,本发明的示例性目的是提供用于有效地确保ProSe中的直接通信的安全的解决方案。

[0015] 用于解决问题的方案

[0016] 为了实现上述目的,根据本发明的第一典型方面的UE包括:获取部件,用于在所述UE成功地登记至节点时,从所述节点获取根密钥,其中所述节点支持所述UE和所述UE附近的允许与所述UE进行通信的一个或多个不同UE之间的直接通信;以及得出部件,用于通过使用所述根密钥其中之一来得出用以与所述不同UE中的一个UE安全地进行直接通信的一对会话密钥。

[0017] 此外,根据本发明的第二典型方面的节点支持彼此邻近的允许彼此进行通信的多个UE之间的直接通信。所述节点包括:获取部件,用于在所述多个UE中的一个UE成功地登记至所述节点时从服务器获取根密钥,其中所述多个UE中的所述一个UE使用所述根密钥来得出用以与所述多个UE中的至少一个其它UE安全地进行直接通信的一对会话密钥,所述服务器管理所述根密钥;以及分发部件,用于将所述根密钥分发给所述多个UE中的所述一个UE。

[0018] 此外,根据本发明的第三典型方面的服务器包括:存储部件,用于存储多个UE中的各UE的用以得出一对会话密钥的根密钥,其中所述会话密钥用于与所述多个UE中的至少一个其它UE安全地进行直接通信,所述多个UE彼此邻近并且允许彼此进行通信;以及应答部件,用于通过将所述根密钥发送至节点来应答来自所述节点的请求,其中所述节点支持所述多个UE之间的直接通信。

[0019] 此外,根据本发明的第四典型方面的通信系统包括:多个用户设备即多个UE,所述多个UE彼此邻近并且允许彼此进行直接通信;节点,用于支持所述直接通信;以及服务器,用于管理各UE的用以得出一对会话密钥的根密钥,其中所述会话密钥用于与所述多个UE中的至少一个其它UE安全地进行直接通信。所述节点在所述多个UE中的各UE成功地登记至所述节点时从所述服务器获取所述根密钥,并且将所获取的根密钥分发给所述多个UE中的各UE。所述多个UE中的各UE通过使用所分发的根密钥其中之一来得出所述会话密钥。

[0020] 此外,根据本发明的第五典型方面的方法提供一种用于控制UE中的操作的方法。所述方法包括以下步骤:在将所述UE成功地登记至节点时从所述节点获取根密钥,其中所述节点支持所述UE和所述UE附近的允许与所述UE进行通信的一个或多个不同UE之间的直接通信;以及通过使用所述根密钥其中之一,得出用于与所述不同UE中的一个UE安全地进行直接通信的会话密钥。

[0021] 此外,根据本发明的第六典型方面的方法提供一种用于控制节点中的操作的方法,其中所述节点支持彼此邻近的允许彼此进行通信的多个UE之间的直接通信。所述方法包括以下步骤:在所述多个UE中的一个UE成功地登记至所述节点时从服务器获取根密钥,其中所述多个UE中的所述一个UE使用所述根密钥来得出用于与所述多个UE中的至少一个其它UE安全地进行直接通信的一对会话密钥,所述服务器管理所述根密钥;以及将所述根密钥分发给所述多个UE中的所述一个UE。

[0022] 此外,根据本发明的第七典型方面的方法提供一种用于控制服务器中的操作的方法。所述方法包括以下步骤:存储各UE的用以得出一对会话密钥的根密钥,其中所述会话密钥用于与所述多个UE中的至少一个其它UE安全地进行直接通信,所述多个UE彼此邻近并且允许彼此进行通信;以及通过将所述根密钥发送至节点来应答来自所述节点的请求,其中所述节点支持所述多个UE之间的直接通信。

[0023] 此外,根据本发明的第八典型方面的UE包括:第一部件,用于在所述UE成功地登记

至节点时登记所述UE的公钥,并且检索一个或多个不同UE的公钥,其中在所述不同UE与所述UE邻近的情况下允许所述不同UE与所述UE进行直接通信,所述节点支持所述直接通信;以及第二部件,用于通过使用所述不同UE中的第一UE的公钥来验证来自所述第一UE的用以与所述UE进行直接通信的请求,其中所述请求是由所述第一UE的私钥所保护的。

[0024] 此外,根据本发明的第九典型方面的UE包括:第一部件,用于在所述UE成功地登记至节点时登记所述UE的公钥,并且检索一个或多个不同UE的公钥,其中在所述不同UE与所述UE邻近的情况下允许所述不同UE与所述UE进行直接通信,所述节点支持所述直接通信;以及第二部件,用于通过使用所述不同UE中的第一UE的公钥来验证针对用于请求所述第一UE与所述UE进行一对一直接通信的受保护的第一请求的应答,其中所述应答是由所述第一UE的私钥所保护的。

[0025] 此外,根据本发明的第十典型方面的节点支持彼此邻近的允许彼此进行通信的多个UE之间的直接通信。所述节点包括:接收部件,用于在所述多个UE中的一个UE成功地登记至所述节点时从所述多个UE中的所述一个UE接收公钥;以及发送部件,用于向所述多个UE中的所述一个UE发送其它UE的公钥作为针对成功登记的应答。所述多个UE中的各UE使用所述公钥来至少验证针对所述直接通信的请求。

[0026] 此外,根据本发明的第十一典型方面的服务器包括:存储部件,用于存储多个UE的公钥,其中在所述多个UE彼此邻近的情况下允许所述多个UE彼此进行直接通信,所述公钥通过支持所述直接通信的节点来进行登记;以及应答部件,用于通过将所存储的公钥发送至所述节点来应答来自所述节点的请求。所述多个UE中的各UE使用所述公钥来至少验证针对所述直接通信的请求。

[0027] 此外,根据本发明的第十二典型方面的通信系统包括:多个用户设备即多个UE,其中在所述多个UE彼此邻近的情况下允许所述多个UE彼此进行直接通信;以及节点,用于支持所述直接通信。所述多个UE中的各UE在所述多个UE中的各UE成功地登记至所述节点时经由所述节点来共享所述多个UE的公钥,并且通过使用所述公钥其中之一来至少验证针对所述直接通信的请求。所述节点在所述多个UE中的各UE登记至所述节点时从所述多个UE中的各UE接收所述公钥中的各公钥,并且向所述多个UE中的各UE发送不同UE的公钥作为针对成功登记的应答。

[0028] 此外,根据本发明的第十三典型方面的方法提供一种用于控制UE中的操作的方法。所述方法包括以下步骤:在所述UE成功地登记至节点时登记所述UE的公钥,并且检索一个或多个不同UE的公钥,其中在所述不同UE与所述UE邻近的情况下允许所述不同UE与所述UE进行直接通信,所述节点支持所述直接通信;以及通过使用所述不同UE中的第一UE的公钥来验证来自所述第一UE的用以与所述UE进行直接通信的请求,其中所述请求是由所述第一UE的私钥所保护的。

[0029] 此外,根据本发明的第十四典型方面的方法提供一种用于控制UE中的操作的方法。所述方法包括以下步骤:在所述UE成功地登记至节点时登记所述UE的公钥,并且检索一个或多个不同UE的公钥,其中在所述不同UE与所述UE邻近的情况下允许所述不同UE与所述UE进行直接通信,所述节点支持所述直接通信;以及通过使用所述不同UE中的第一UE的公钥来验证针对用于请求所述第一UE与所述UE进行一对一直接通信的受保护的请求的应答,其中所述应答是由所述第一UE的私钥所保护的。

[0030] 此外,根据本发明的第十五典型方面的方法提供一种节点的控制方法,其中所述节点支持彼此邻近的允许彼此进行通信的多个UE之间的直接通信。所述控制方法包括以下步骤:在所述多个UE中的一个UE成功地登记至所述节点时,从所述多个UE中的所述一个UE接收公钥;以及向所述多个UE中的所述一个UE发送其它UE的公钥作为针对成功登记的应答。所述多个UE中的各UE使用所述公钥来至少验证针对所述直接通信的请求。

[0031] 此外,根据本发明的第十六典型方面的方法提供一种用于控制服务器中的操作的方法。所述方法包括以下步骤:存储多个UE的公钥,其中在所述多个UE彼此邻近的情况下允许所述多个UE彼此进行直接通信,所述公钥通过支持所述直接通信的节点来进行登记;以及通过将所存储的公钥发送至所述节点来应答来自所述节点的请求。所述多个UE中的各UE使用所述公钥来至少验证针对所述直接通信的请求。

[0032] 发明的效果

[0033] 根据本发明,可以解决上述的问题,因而可以提供用于有效地确保ProSe中的直接通信的安全的解决方案。

[0034] 例如,根据第一至第七典型方面任何之一,可以实现以下有利效果。

[0035] 1)中央根密钥管理,防止了同步问题。

[0036] 2)每当UE需要直接通信服务的情况下,减少根分配。

附图说明

[0037] 图1是示出根据本发明的第一典型实施例的通信系统的结构示例的框图。

[0038] 图2是示出根据第一典型实施例的用于在通信系统中分配根密钥的操作的示例的顺序图。

[0039] 图3是示出根据第一典型实施例的用于在通信系统中分配根密钥的操作的另一示例的顺序图。

[0040] 图4是示出根据第一典型实施例的用于在通信系统中得出会话密钥的操作的示例的顺序图。

[0041] 图5是示出根据第一典型实施例的用于在通信系统中得出会话密钥的操作的另一示例的顺序图。

[0042] 图6是示出根据第一典型实施例的UE的结构示例的框图。

[0043] 图7是示出根据第一典型实施例的节点的结构示例的框图。

[0044] 图8是示出根据第一典型实施例的服务器的结构示例的框图。

[0045] 图9是示出根据本发明的第二典型实施例的通信系统的结构示例的框图。

[0046] 图10是示出根据第二典型实施例的用于在通信系统中登记UE的操作的示例的顺序图。

[0047] 图11是示出根据第二典型实施例的用于在通信系统中得出一对一直接通信所用的会话密钥的操作的示例的顺序图。

[0048] 图12是示出根据第二典型实施例的用于在通信系统中得出一对多直接通信所用的会话密钥的操作的示例的顺序图。

[0049] 图13是示出根据第二典型实施例的UE的结构示例的框图。

[0050] 图14是示出根据第二典型实施例的节点的结构示例的框图。

[0051] 图15是示出根据第二典型实施例的服务器的结构示例的框图。

具体实施方式

[0052] 以下,将参考附图来说明根据本发明的UE、节点和服务器以及这些UE、节点和服务器所应用至的通信系统的第一典型实施例和第二典型实施例。

[0053] 第一典型实施例

[0054] 图1示出邻近服务所用的通信系统的结构示例。邻近服务提供了针对商业/社会使用和公共安全使用这两者的由运营商网络控制的发现和邻近的UE之间的通信。要求应当在存在网络覆盖或不存在网络覆盖的情况下向UE提供ProSe服务。

[0055] 如图1所示,根据本典型实施例的通信系统包括:多个UE 10_1～10_m(以下可以利用附图标记10统一指代);一个或多个ProSe功能体20_1～20_n(以下可以利用附图标记20统一指代);E-UTRAN(Evolved Universal Terrestrial Radio Access Network,演进型通用陆地无线接入网)30;EPC(Evolved Packet Core,演进型分组核心)40;以及ProSe APP(应用程序)服务器50。

[0056] UE 10经由E-UTRAN 30(即,经由接口LTE-Uu和S1)附着至EPC 40,由此用作典型UE。此外,UE 10使用上述的接口PC5,由此进行ProSe通信。在进行ProSe通信之前,UE 10向ProSe功能体20进行登记。注意,UE 10_1～10_m可以向同一ProSe功能体或者相互不同的ProSe功能体进行登记。此外,UE 10_1～10_m中的一部分可以向同一ProSe功能体进行登记。

[0057] ProSe功能体20是支持UE 10_1～10_m之间的ProSe通信的节点。ProSe功能体20可以部署在特定网络节点中或者可以是独立节点,并且可以驻留在EPC 40以内或以外。ProSe功能体20经由接口PC3与UE 10进行通信。此外,ProSe功能体20经由接口PC4与EPC 40进行通信。此外,ProSe功能体20_1～20_n可以经由接口PC6与彼此进行通信。

[0058] 注意,接口PC3是UE 10和ProSe功能体20之间的参考点。使用接口PC3来定义UE 10和ProSe功能体20之间的交互。一个示例可以是用于针对ProSe发现和通信的配置。此外,接口PC4是EPC 40和ProSe功能体20之间的参考点。使用接口PC4来定义EPC 40和ProSe功能体20之间的交互。可能的用例可以是在UE 10_1～10_m之间建立一对一通信路径的情况或者是针对实时会话管理或移动管理来验证ProSe服务(授权)的情况。此外,接口PC6是ProSe功能体20_1～20_n之间的参考点。可以针对诸如与不同的PLMN(Public Land Mobile Network,公共陆地移动网络)签约的用户之间的ProSe发现等的功能使用接口PC6。

[0059] E-UTRAN 30包括一个或多个eNB(演进型Node B)(未示出)。EPC 40包括用于管理UE 10_1～10_m的移动的MME(移动管理实体)等作为EPC 40的网络节点。ProSe APP服务器50可以经由接口SGi与EPC 40进行通信。此外,ProSe APP服务器50可以经由接口PC1与UE 10进行通信,并且可以经由接口PC2与ProSe功能体20进行通信。注意,接口PC1是UE 10_1～10_m中的ProSe APP与ProSe APP服务器50之间的参考点。使用接口PC1来定义应用层信令要求。另一方面,接口PC2是ProSe功能体20与ProSe APP服务器50之间的参考点。使用接口PC2来定义ProSe APP服务器50与3GPP EPS(Evolved Packet System,演进型分组系统)经由ProSe功能体20所提供的ProSe功能之间的交互。一个示例可以用于针对ProSe功能体20中的ProSe数据库的应用程序数据更新。另一示例可以是ProSe APP服务器50所使用的在

3GPP功能与应用程序数据之间互通的数据,例如,名称翻译。ProSe APP服务器50可以驻留在EPC 40以内或以外。

[0060] 尽管省略了例示,但通信系统还包括由信任的第三方操作的服务器。在以下说明中,该服务器有时将被简称为“第三(第3)方”,并且由附图标记60所指代。通常,第三方60管理后面将说明的根密钥。

[0061] 接着,将参考图2～5详细说明本典型实施例的操作示例。注意,后面将参考图6和8说明UE 10、ProSe功能体20和第三方60的结构示例。

[0062] 本典型实施例提出使用第三方60来得出、更新并分配根密钥。ProSe功能体20支持直接通信并且在UE 10登记时向该UE 10分配所有的根密钥。通过使用根密钥在UE 10侧得出会话密钥。例如,会话密钥是用于保护在UE 10_1～10_m之间直接传送的消息的一对加密密钥和完整性密钥。

[0063] 用于分配根密钥的操作

[0064] 针对根密钥分配提出两个选项。

[0065] 选项1:根密钥与给定UE相关

[0066] 根密钥在登记时进行得出和分配。假定ProSe功能体20具有允许与UE 10_1进行通信的UE的列表,并且ProSe功能体20可以从信任的第三方60索要UE 10_1所用的所有根密钥。第三方60负责密钥得出和分配。ProSe功能体20_1～20_n可以从第三方60中检索登记至ProSe功能体20_1～20_n的UE 10_1～10_m所用的根密钥,以使得无需在ProSe功能体20_1～20_n之间进行同步。各根密钥通过唯一KSI(密钥集标识符)进行标识。在发生直接通信的情况下,ProSe功能体20可以向UE 10_1～10_m指示要使用哪个KSI,或者UE 10_1～10_m可以对此进行协商。

[0067] 具体地,如图2所示,UE 10_1在ProSe功能体20_1处进行登记(步骤S11)。

[0068] ProSe功能体20_1将请求UE 10_1所用的根密钥发送至管理根密钥的第三方60(步骤S12)。

[0069] 第三方60利用UE 10_1所用的根密钥来应答ProSe功能体20_1。各根密钥与唯一KSI以及允许UE 10_1享有ProSe服务的UE相关(步骤S13)。

[0070] ProSe功能体20_1向UE 10_1分发包括UE ID和KSI的根密钥(步骤S14)。

[0071] 在UE 10_2与ProSe功能体20_2之间进行与步骤S11～S14相同的过程(步骤S15～S18)。

[0072] 选项2:根密钥池

[0073] 与选项1类似,UE可以获得密钥池,其中在该密钥池中,各密钥具有用以标识出该密钥的唯一KSI。在UE 10_1需要直接通信所用的会话密钥的情况下,网络(ProSe功能体)可以指示要使用哪个密钥,并且还针对UE 10_1和UE 10_2给出相同的参数以使得UE 10_1和UE 10_2可以得出相同的会话密钥。

[0074] 与选项1相比的不同之处在于:这里,根密钥不与任何UE相关。因此,ProSe功能体20需要确保相同的根密钥将不会被不同的UE再使用。

[0075] 具体地,如图3所示,UE 10_1在ProSe功能体20_1处进行登记(步骤S21)。

[0076] ProSe功能体20_1将请求UE 10_1所用的根密钥发送至管理根密钥的第三方60(步骤S22)。

[0077] 第三方60利用包括多个根密钥的根密钥池来应答ProSe功能体20_1。各密钥与唯一KSI相关(步骤S23)。

[0078] ProSe功能体20_1向UE 10_1分发具有KSI的根密钥(步骤S24)。

[0079] 在UE 10_2与ProSe功能体20_2之间进行与步骤S21～S24相同的过程(步骤S25～S28)。

[0080] 根据本选项2,可以与选项1相比减少针对UE的信令量。这是由于根密钥不与任何UE相关,因而与选项1相比,发送至UE的根密钥的数量可以更少。此外,还可以减少UE中用于存储根密钥的资源。

[0081] 与此相对,根据选项1,可以与选项2相比减少ProSe功能体的负荷。这是由于根密钥是以一对一的方式分配给UE的,因而ProSe功能体不需要确保相同的根密钥将不会被不同的UE再使用。

[0082] 用于得出会话密钥的操作

[0083] 针对会话密钥得出和分配提出两个选项。

[0084] 选项1:UE自主得出会话密钥

[0085] 发起直接通信的UE 10_1简单地得出会话密钥,将该会话密钥发送至ProSe功能体,并且ProSe功能体将向其它UE发送该会话密钥。

[0086] 可选地,如图4所示,UE 10_1向UE 10_2发送直接通信(Direct Communication)请求(步骤S31)。

[0087] 在如图2所示各根密钥与给定UE相关的情况下,UE 10_1和10_2可以在没有从网络接收到任何指示的情况下识别出要用于得出会话密钥的相同的根密钥。因此,UE 10_1和10_2独立地根据所识别出的根密钥得出会话密钥(步骤S32)。

[0088] 然后,UE 10_1和10_2在通过使用会话密钥进行安全保护的情况下开始进行直接通信(步骤S33)。

[0089] 选项2:UE根据ProSe功能体所指示的KSI得出会话密钥

[0090] 本选项适用于如图3所示对根密钥池进行分配的情况。

[0091] 如图5所示,UE 10_1将具有UE 10_2(UE 10_1想要享有与该UE的直接通信服务)的ID的直接通信请求发送至ProSe功能体20_1(步骤S41)。

[0092] ProSe功能体20_1针对是否允许UE 10_1与UE 10_2进行直接通信进行授权(步骤S42)。

[0093] 在成功授权的情况下,ProSe功能体20_1向UE 10_1指示根密钥KSI(步骤S43)。

[0094] 此外,ProSe功能体20_1经由ProSe功能体20_2向UE 10_2指示该根密钥KSI(步骤S44)。

[0095] UE 10_1和UE 10_2单独地根据KSI所指示的根密钥得出会话密钥(步骤S45)。

[0096] 然后,UE 10_1和UE 10_2在通过使用会话密钥进行安全保护的情况下开始进行直接通信(步骤S46)。

[0097] 接着,将参考图6～8说明根据本典型实施例的UE 10、ProSe功能体(节点)20和第三方(服务器)60的结构示例。

[0098] 如图6所示,UE 10包括获取单元11和得出单元12。在成功地向ProSe功能体20登记了UE 10的情况下,获取单元11从ProSe功能体20获取根密钥。得出单元12通过使用所获取

的根密钥得出会话密钥。在如图2所示各根密钥与给定UE相关的情况下,得出单元12在得出会话密钥时使用与UE 10期望进行直接通信的UE相对应的根密钥。另一方面,在如图3所示对根密钥池进行分配的情况下,得出单元12使用从ProSe功能体20接收到的KSI所指示的根密钥。注意,这些单元11和12经由总线等与彼此相互连接。这些单元11和12例如可以包括:经由接口PC5与不同的UE进行直接通信的收发器;经由接口PC3与ProSe功能体20进行通信的收发器;以及诸如CPU(中央处理单元)等的控制这些收发器的控制器。

[0099] 如图7所示,ProSe功能体20包括获取单元21和分发单元22。在成功地向ProSe功能体20登记了UE 10的情况下,获取单元21从第三方60获取根密钥。分发单元22将所获取的根密钥分发给UE 10。在如图3所示对根密钥池进行分配的情况下,ProSe功能体20还包括指示单元23。指示单元23向UE 10指示UE 10要使用的根密钥的KSI。注意,这些单元21～23经由总线等与彼此相互连接。这些单元21～23例如可以包括经由接口PC3与UE 10进行通信的收发器以及诸如CPU等的控制该收发器的控制器。

[0100] 如图8所示,第三方60包括存储单元61和应答单元62。存储单元61存储根密钥。应答单元62通过将根密钥发送至ProSe功能体20来应答来自ProSe功能体20的请求。注意,这些单元61和62经由总线等与彼此相互连接。这些单元61和62例如可以包括与ProSe功能体20进行通信的收发器以及诸如CPU等的控制该收发器的控制器。

[0101] 第二实施例

[0102] 图9示出邻近服务所用的通信系统的结构示例。邻近服务提供针对商业/社会使用和公共安全使用这两者的由运营商网络控制的发现和邻近的UE之间的通信。要求应当在存在网络覆盖或不存在网络覆盖的情况下向UE提供ProSe服务。

[0103] 如图9所示,根据本典型实施例的通信系统包括多个UE 110_1～110_m(以下可以利用附图标记110统一指代)、一个或多个ProSe功能体120_1～120_n(以下可以利用附图标记120统一指代)、E-UTRAN(Evolved Universal Terrestrial Radio Access Network,演进型通用陆地无线接入网)130、EPC(Evolved Packet Core,演进型分组核心)140、以及ProSe APP(应用程序)服务器150。

[0104] UE 110经由E-UTRAN 130(即,经由接口LTE-Uu和S1)附着至EPC 140,由此用作典型UE。此外,UE 110使用上述的接口PC5,由此进行ProSe通信。在进行ProSe通信之前,UE 110向ProSe功能体120进行登记。注意,UE 110_1～110_m可以向同一ProSe功能体或者相互不同的ProSe功能体进行登记。此外,UE 110_1～110_m中的一部分可以向同一ProSe功能体进行登记。

[0105] ProSe功能体120是支持UE 110_1～110_m之间的ProSe通信的节点。ProSe功能体120可以部署在特定网络节点中或者可以是独立节点,并且可以驻留在EPC 140以内或以外。ProSe功能体120经由接口PC3与UE 110进行通信。此外,ProSe功能体120经由接口PC4与EPC 140进行通信。此外,ProSe功能体120_1～120_n可以经由接口PC6与彼此进行通信。

[0106] 注意,接口PC3是UE 110和ProSe功能体120之间的参考点。使用接口PC3来定义UE 110和ProSe功能体120之间的交互。一个示例可以是用于ProSe发现和通信的配置。此外,接口PC4是EPC 140和ProSe功能体120之间的参考点。使用接口PC4来定义EPC 140和ProSe功能体120之间的交互。可能的用例可以是在UE 110_1～110_m之间建立一对一通信路径的情况或者是针对实时会话管理或移动管理来验证ProSe服务(授权)的情况。此外,接口PC6是

ProSe功能体120_1～120_n之间的参考点。可以针对诸如与不同的PLMN(Public Land Mobile Network,公共陆地移动网络)签约的用户之间的ProSe发现等的功能使用接口PC6。

[0107] E-UTRAN 130包括一个或多个eNB(未示出)。EPC 140包括管理UE 110_1～110_m的移动的MME(移动管理实体)等作为EPC 140的网络节点。ProSe APP服务器150可以经由接口SGi与EPC 140进行通信。此外,ProSe APP服务器150可以经由接口PC1与UE 110进行通信,并且可以经由接口PC2与ProSe功能体120进行通信。注意,接口PC1是UE 110_1～110_m中的ProSe APP与ProSe APP服务器150之间的参考点。使用接口PC1来定义应用层信令要求。另一方面,接口PC2是ProSe功能体120与ProSe APP服务器150之间的参考点。使用接口PC2来定义ProSe APP服务器150与3GPP EPS(演进型分组系统)经由ProSe功能体120所提供的ProSe功能之间的交互。一个示例可以用于针对ProSe功能体120中的ProSe数据库的应用程序数据更新。另一示例可以是ProSe APP服务器150所使用的在3GPP功能与应用程序数据之间互通的数据,例如,名称翻译。ProSe APP服务器150可以驻留在EPC 140以内或以外。

[0108] 尽管省略了例示,但通信系统还包括由信任的第三方操作的服务器。在以下说明中,该服务器有时将被简称为"第三(第3)方"并且由附图标记160所指代。通常,第三方160管理后面将说明的公钥。

[0109] 接着,将参考图10～12详细说明本典型实施例的操作示例。注意,后面将参考图13～15说明UE 110、ProSe功能体120和第三方160的结构示例。

[0110] 本典型实施例提出使用PKI来进行直接通信。UE 110_1～UE 110_m可以在登记过程中登记它们的公钥并且同时获得其它UE的公钥。ProSe功能体120确保仅向UE 110提供如下UE的公钥,其中允许发出请求的UE 110与该UE进行直接通信。UE 110_1～UE 110_m使用公钥来验证另一端,以使得UE 110_1～UE 110_m可以得出会话密钥,从而开始进行直接通信。例如,会话密钥是用于保护在UE 110_1～110_m之间直接传送的消息的一对加密密钥和完整性密钥。

[0111] 以下,给出针对密钥得出的选项。

[0112] 1.使用PKI来进行一对一直接通信:

[0113] UE 110_1～UE 110_m在登记时提供它们的公钥并且在登记成功的情况下接收其它UE的公钥。例如,UE 110_1利用其私钥来保护直接通信请求。接收到直接通信请求的UE110_2可以利用UE1的公钥来验证该直接通信请求。UE 110_2可以将会话密钥得出所用的材料发送至UE 110_1并且UE 110_2和UE 110_1可以得出相同的密钥来保护它们的直接通信。UE 110_1可以利用UE2的公钥来验证从UE 110_2发送来的消息,由此UE 110_1和UE 110_2可以互相认证。

[0114] 会话密钥得出可以:

[0115] 1)使用预先从ProSe功能体获取的具有UE其中之一为了保持新鲜度而提供的密钥材料的根密钥,作为输入;以及

[0116] 2)还使用密钥交换方案(例如,Diffie-Hellman密钥交换方案)来计算和共享私密密钥。

[0117] 具体地,如图10所示,UE 110_1在向ProSe功能体120_1登记期间,登记该UE 110_1的公钥(步骤S111)。

[0118] ProSe功能体120_1将UE 110_1的公钥登记在第三方160中(步骤S112)。

[0119] 第三方160向ProSe功能体120_1发送允许列表。该允许列表包含允许UE 110_1进行直接通信的UE的ID以及这些UE的相关公钥(步骤S113)。

[0120] ProSe功能体120_1将允许列表转发至UE 110_1(步骤S114)。

[0121] 针对UE 110_2进行与步骤S111～S114相同的过程(步骤S115～S118)。

[0122] 在直接通信开始的情况下,如图11所示,UE 110_1向ProSe功能体120_1发送具有UE 110_2的ID、UE 110_1的公钥KSI的直接通信请求。可以利用UE 110_1的私钥来保护消息。该消息由ProSe功能体120_1转发至ProSe功能体120_2(步骤S121)。

[0123] 注意,KSI的使用适用于向UE 110_1分配多个公钥的情况。UE 110_2可以参考KSI来识别与UE 110_1所使用的私钥相对应的公钥其中之一。

[0124] ProSe功能体120_1在ProSe功能体120_2的支持下对UE 110_1是否可以享有与UE 110_2的直接通信服务进行授权(步骤S122)。

[0125] 在成功授权的情况下,ProSe功能体120_2向UE 110_2发送直接通信请求(步骤S123)。

[0126] 注意,如果在UE超出覆盖范围的情况下发生直接通信,则直接通信请求从UE 110_1直接到达UE 110_2,并且省略以上的步骤S122。

[0127] UE 110_2可以利用UE 110_1的公钥对消息进行完整性检查(步骤S124)。

[0128] 在完整性检查成功的情况下,UE 110_2如上所述得出会话密钥(步骤S125)。

[0129] UE 110_2向UE 110_1发送具有会话密钥得出所用的材料的直接通信应答。可选地,UE 110_2将所得出的会话密钥包括在直接通信应答中。利用UE 110_2的私钥来保护消息(步骤S126)。

[0130] UE 110_1利用UE 110_2的公钥对消息进行完整性检查(步骤S127)。

[0131] 在完整性检查成功的情况下,UE 110_1根据材料得出会话密钥(步骤S128)。如果在步骤S126中UE 110_1从UE 110_2接收到会话密钥,则跳过该步骤S128。可选地,UE 110_1通过使用UE 110_2的公钥从直接通信应答中提取会话密钥。

[0132] 此后,在通过UE 110_1和UE 110_2所共享的会话密钥进行安全保护的情况下开始进行直接通信(步骤S129)。

[0133] 2.使用PKI来进行一对多直接通信:

[0134] 登记过程与图10所示相同。

[0135] UE 110_1利用其私钥来保护直接通信请求。其它UE(例如,UE 110_2、UE 110_3)可以利用UE1的公钥来验证该直接通信请求。

[0136] 另一方面,在本选项中,UE 110_1得出一对多直接通信所用的会话密钥,并且将会话密钥与直接通信请求一起经由安全接口PC3发送至ProSe功能体120。ProSe功能体120向UE 110_2和UE 110_3发送会话密钥。如果UE 110_2或UE 110_3已向不同的ProSe功能体进行了登记,则UE 110_1的ProSe功能体将向UE 110_2/UE 110_3的服务ProSe功能体转发会话密钥。会话密钥得出可以使用UE 110_1的私钥或者任何LTE(长期演进)密钥作为输入。

[0137] 具体地,如图12所示,UE 110_1得出直接通信所用的会话密钥(步骤S131)。

[0138] UE 110_1向ProSe功能体120_1发送直接通信请求,其中该直接通信请求可以转发至用于服务目标UE的ProSe功能体(例如,ProSe功能体20_2,以及UE 110_2和110_3)。消息包含由UE 110_1的私钥所保护的目标UE的ID和UE 110_1的公钥KSI。UE 110_1还将会话密

钥包括在该消息中(步骤S132)。

[0139] ProSe功能体120_1和120_2对UE 110_1是否可以与目标UE 110_2和110_3进行一对多直接通信进行授权(步骤S133)。

[0140] ProSe功能体120_2将直接通信请求转发至UE 110_2和110_3(步骤S134)。

[0141] UE 110_2和110_3各自利用UE 110_1的公钥对消息进行完整性检查(步骤S135)。

[0142] UE 110_2和110_3各自向UE 110_1发送由所接收到的会话密钥所保护的直接通信应答(步骤S136)。此后,在通过UE 110_1～UE 110_3所共享的会话密钥进行安全保护的情况下开始进行直接通信。

[0143] 3.使用PKI来进行不使用会话密钥的一对多直接通信:

[0144] 考虑到一对多通信是仅从UE1到其它的单向通信,UE 110_1简单地利用其私钥来保护至其它UE的直接通信。授权从UE 110_1接收消息的其它UE可以得到UE 110_1的公钥,由此验证出消息是从UE 110_1发送来的并且读取该消息。网络(例如,ProSe功能体)应确保未经授权的UE将不会得到UE 110_1的公钥并且不应将该公钥发送至其它UE。

[0145] 因而,可以(如非专利文献2第5.12条所要求的那样)防止非成员收听ProSe组通信传输。

[0146] 4.使用PKI将一对多公钥作为输入:

[0147] UE 110_1～110_m得出会话密钥,并且密钥得出的输入为:1)UE 110_1的公钥;2)从ProSe功能体120接收到的密钥得出材料。要求仅向授权UE提供UE 110_1的公钥和密钥得出材料。

[0148] UE 110_1如何具有相同的会话密钥:

[0149] a)UE 110_1保持公钥并且从ProSe功能体120接收密钥得出材料,以使得UE 110_1可以以相同的会话密钥得出会话;

[0150] b)由于ProSe功能体120获知UE 110_1的公钥和密钥得出材料这两者,因此ProSe功能体120可以得出密钥;

[0151] c)ProSe功能体120提供密钥得出材料,其中UE 110_1可以将该密钥得出材料与UE 110_1的私钥一起使用,以得出相同的会话密钥。

[0152] 这要求针对UE 110_1的密钥得出材料和针对其它UE的密钥得出材料具有某种关系。

[0153] 接着,将参考图13～15说明根据本典型实施例的UE 110、ProSe功能体(节点)120和第三方(服务器)160的结构示例。

[0154] 如图13所示,UE 110包括登记/检索单元111和验证单元112。登记/检索单元111进行图10所示的处理或者与图10所示的处理等价的处理。验证单元112进行图11和12所示的处理或者与图11和12所示的处理等价的处理。注意,这些单元111和112经由总线等与彼此相互连接。这些单元111和112例如可以包括:经由接口PC5与不同的UE进行直接通信的收发器;经由接口PC3与ProSe功能体120进行通信的收发器;以及诸如CPU(中央处理单元)等的控制这些收发器的控制器。

[0155] 如图14所示,ProSe功能体120至少包括接收单元121和发送单元122。接收单元121进行图10中的步骤S111和S115所示的处理或者与图10中的步骤S111和S115所示的处理等价的处理。发送单元122进行图10中的步骤S114和S118所示的处理或者与图10中的步骤

S114和S118所示的处理等价的处理。此外,ProSe功能体120还可以包括登记单元123和获取单元124。登记单元123进行图10中的步骤S112和S116所示的处理或者与图10中的步骤S112和S116所示的处理等价的处理。获取单元124进行图10中的步骤S113和S117所示的处理或者与图10中的步骤S113和S117所示的处理等价的处理。注意,这些单元121～124经由总线等与彼此相互连接。这些单元121～124例如可以包括经由接口PC3与UE 110进行通信的收发器;与第三方160进行通信的收发器;以及诸如CPU等的控制这些收发器的控制器。

[0156] 如图15所示,第三方160包括存储单元161和应答单元162。存储单元161存储ProSe功能体120所登记的根密钥。应答单元162通过将所存储的公钥发送至ProSe功能体120来应答来自ProSe功能体120的请求。注意,这些单元161和162经由总线等与彼此相互连接。这些单元161和162例如可以包括与ProSe功能体120进行通信的收发器以及诸如CPU等的控制该收发器的控制器。

[0157] 注意,本发明不限于上述的典型实施例,并且本领域普通技术人员可以基于权利要求书的记载进行各种修改,这是显而易见的。

[0158] 以上公开的典型实施例的整体或一部分可以被描述为但不限于以下附注。

[0159] 附注1

[0160] 一种用户设备即UE,包括:

[0161] 获取部件,用于在所述UE成功地登记至节点时,从所述节点获取根密钥,其中所述节点支持所述UE和所述UE附近的允许与所述UE进行通信的一个或多个不同UE之间的直接通信;以及

[0162] 得出部件,用于通过使用所述根密钥其中之一来得出用以与所述不同UE中的一个UE安全地进行直接通信的一对会话密钥。

[0163] 附注2

[0164] 根据附注1所述的UE,所述根密钥以一一对应的方式与所述不同UE相关,以及所述得出部件被配置为在得出所述会话密钥的情况下,使用与所述不同UE中的所述一个UE相对应的根密钥。

[0165] 附注3

[0166] 根据附注1所述的UE,所述根密钥是与给定UE不相关的多个密钥,以及所述得出部件被配置为在得出所述会话密钥的情况下,使用所述节点所指示的根密钥。

[0167] 附注4

[0168] 根据附注1～3中任一项所述的UE,所述直接通信包括ProSe通信即基于邻近的服务的通信。

[0169] 附注5

[0170] 一种节点,用于支持彼此邻近的允许彼此进行通信的多个UE之间的直接通信,所述节点包括:

[0171] 获取部件,用于在所述多个UE中的一个UE成功地登记至所述节点时从服务器获取根密钥,其中所述多个UE中的所述一个UE使用所述根密钥来得出用以与所述多个UE中的至少一个其它UE安全地进行直接通信的一对会话密钥,所述服务器管理所述根密钥;以及

[0172] 分发部件,用于将所述根密钥分发给所述多个UE中的所述一个UE。

[0173] 附注6

[0174] 根据附注5所述的节点,其中,所述根密钥以一一对应的方式与相互不同的UE相关。

[0175] 附注7

[0176] 根据附注5所述的节点,其中,还包括:

[0177] 指示部件,用于在所述根密钥是与给定UE不相关的多个密钥的情况下向所述UE中的所述一个UE指示要使用哪个根密钥来得出所述会话密钥。

[0178] 附注8

[0179] 根据附注4~7中任一项所述的节点,其中,所述直接通信包括ProSe通信。

[0180] 附注9

[0181] 一种服务器,包括:

[0182] 存储部件,用于存储多个UE中的各UE的用以得出一对会话密钥的根密钥,其中所述会话密钥用于与所述多个UE中的至少一个其它UE安全地进行直接通信,所述多个UE彼此邻近并且允许彼此进行通信;以及

[0183] 应答部件,用于通过将所述根密钥发送至节点来应答来自所述节点的请求,其中所述节点支持所述多个UE之间的直接通信。

[0184] 附注10

[0185] 根据附注9所述的服务器,其中,所述根密钥以一一对应的方式与相互不同的UE相关。

[0186] 附注11

[0187] 根据附注9所述的服务器,其中,所述根密钥是与给定UE不相关的多个密钥。

[0188] 附注12

[0189] 根据附注9~11中任一项所述的服务器,其中,所述直接通信包括ProSe通信。

[0190] 附注13

[0191] 一种通信系统,包括:

[0192] 多个UE,所述多个UE彼此邻近并且允许彼此进行直接通信;

[0193] 节点,用于支持所述直接通信;以及

[0194] 服务器,用于管理各UE的用以得出一对会话密钥的根密钥,其中所述会话密钥用于与所述多个UE中的至少一个其它UE安全地进行直接通信,

[0195] 其中,所述节点在所述多个UE中的各UE成功地登记至所述节点时从所述服务器获取所述根密钥,并且将所获取的根密钥分发给所述多个UE中的各UE,以及

[0196] 所述多个UE中的各UE通过使用所分发的根密钥其中之一来得出所述会话密钥。

[0197] 附注14

[0198] 一种用于控制UE中的操作的方法,所述方法包括以下步骤:

[0199] 在所述UE成功地登记至节点时从所述节点获取根密钥,其中所述节点支持所述UE和允许与所述UE进行通信的一个或多个不同UE之间的直接通信;以及

[0200] 通过使用所述根密钥其中之一来得出用以与所述不同UE中的一个UE安全地进行直接通信的会话密钥。

[0201] 附注15

[0202] 一种用于控制节点中的操作的方法,所述节点支持彼此邻近的允许彼此进行通信

的多个UE之间的直接通信,所述方法包括以下步骤:

[0203] 在所述多个UE中的一个UE成功地登记至所述节点时从服务器获取根密钥,其中所述多个UE中的所述一个UE使用所述根密钥来得出用于与所述多个UE中的至少一个其它UE安全地进行直接通信的一对会话密钥,所述服务器管理所述根密钥;以及

[0204] 将所述根密钥分发给所述多个UE中的所述一个UE。

[0205] 附注16

[0206] 一种用于控制服务器中的操作的方法,所述方法包括以下步骤:

[0207] 存储各UE的用以得出一对会话密钥的根密钥,其中所述会话密钥用于与所述多个UE中的至少一个其它UE安全地进行直接通信,所述多个UE彼此邻近并且允许彼此进行通信;以及

[0208] 通过将所述根密钥发送至节点来应答来自所述节点的请求,其中所述节点支持所述多个UE之间的直接通信。

[0209] 附注17

[0210] 一种用户设备即UE,包括:

[0211] 第一部件,用于在所述UE成功地登记至节点时登记所述UE的公钥,并且检索一个或多个不同UE的公钥,其中在所述不同UE与所述UE邻近的情况下允许所述不同UE与所述UE进行直接通信,所述节点支持所述直接通信;以及

[0212] 第二部件,用于通过使用所述不同UE中的第一UE的公钥来验证来自所述第一UE的用以与所述UE进行直接通信的请求,其中所述请求是由所述第一UE的私钥所保护的。

[0213] 附注18

[0214] 根据附注17所述的UE,其中,

[0215] 所述请求用于请求所述UE与所述第一UE进行一对一直接通信,以及

[0216] 所述第二部件被配置为:

[0217] 在验证成功时,得出用以安全地进行所述一对一直接通信的一对会话密钥;

[0218] 利用所述UE的私钥来保护针对所述请求的应答,其中所述应答包括所述会话密钥或用以得出所述会话密钥的材料;以及

[0219] 将所述应答发送至所述第一UE。

[0220] 附注19

[0221] 根据附注17所述的UE,其中,

[0222] 所述请求用于请求所述UE与所述不同UE中的一个或多个其它UE进行一对多直接通信,并且所述请求包括用以安全地进行所述一对多直接通信的一对会话密钥,以及

[0223] 所述第二部件被配置为从所述请求中提取所述会话密钥。

[0224] 附注20

[0225] 根据附注17~19中任一项所述的UE,其中,

[0226] 向UE分配多个公钥,以及

[0227] 所述第二部件被配置为基于所述请求中所包括的指示来识别所述多个公钥中的进行验证所要使用的公钥。

[0228] 附注21

[0229] 一种用户设备即UE,包括:

[0230] 第一部件,用于在所述UE成功地登记至节点时登记所述UE的公钥,并且检索一个或多个不同UE的公钥,其中在所述不同UE与所述UE邻近的情况下允许所述不同UE与所述UE进行直接通信,所述节点支持所述直接通信;以及

[0231] 第二部件,用于通过使用所述不同UE中的第一UE的公钥来验证针对用于请求所述第一UE与所述UE进行一对一直接通信的受保护的第一请求的应答,其中所述应答是由所述第一UE的私钥所保护的。

[0232] 附注22

[0233] 根据附注21所述的UE,其中,

[0234] 所述应答包括用于安全地进行所述一对一直接通信的一对第一会话密钥或者用于得出所述第一会话密钥的材料,以及

[0235] 所述第二部件被配置为:

[0236] 在验证成功时,从所述应答提取所述第一会话密钥或所述材料;以及

[0237] 在提取到所述材料的情况下,根据所述材料得出所述第一会话密钥。

[0238] 附注23

[0239] 根据附注21或22所述的UE,其中,所述第二部件被配置为:

[0240] 在与所述不同UE中的两个以上UE进行一对多直接通信之前,得出用于安全地进行所述一对多直接通信的一对第二会话密钥;

[0241] 将所述第二会话密钥包括在用于请求所述不同UE中的所述两个以上UE进行所述一对多直接通信的第二请求中;

[0242] 利用所述UE的私钥来保护所述第二请求;以及

[0243] 将所述第二请求经由所述节点发送至所述不同UE中的所述两个以上UE。

[0244] 附注24

[0245] 根据附注21~23中任一项所述的UE,其中,

[0246] 向UE分配多个公钥,以及

[0247] 所述第二部件被配置为将与用于保护所述请求的UE的私钥相对应的公钥的指示包括在所述请求中。

[0248] 附注25

[0249] 一种节点,用于支持彼此邻近的允许彼此进行通信的多个UE之间的直接通信,所述节点包括:

[0250] 接收部件,用于在所述多个UE中的一个UE成功地登记至所述节点时从所述多个UE中的所述一个UE接收公钥;以及

[0251] 发送部件,用于向所述多个UE中的所述一个UE发送其它UE的公钥作为针对成功登记的应答,

[0252] 其中,所述多个UE中的各UE使用所述公钥来至少验证针对所述直接通信的请求。

[0253] 附注26

[0254] 根据附注25所述的节点,其中,还包括:

[0255] 登记部件,用于将所述多个UE中的所述一个UE的公钥登记至服务器;以及

[0256] 获取部件,用于从所述服务器获取所述其它UE的公钥。

[0257] 附注27

[0258] 一种服务器,包括:

[0259] 存储部件,用于存储多个UE的公钥,其中在所述多个UE彼此邻近的情况下允许所述多个UE彼此进行直接通信,所述公钥通过支持所述直接通信的节点来进行登记;以及

[0260] 应答部件,用于通过将所存储的公钥发送至所述节点来应答来自所述节点的请求,

[0261] 其中,所述多个UE中的各UE使用所述公钥来至少验证针对所述直接通信的请求。

[0262] 附注28

[0263] 一种通信系统,包括:

[0264] 多个UE,其中在所述多个UE彼此邻近的情况下允许所述多个UE彼此进行直接通信;以及

[0265] 节点,用于支持所述直接通信,

[0266] 其中,所述多个UE中的各UE在所述多个UE中的各UE成功地登记至所述节点时经由所述节点来共享所述多个UE的公钥,并且通过使用所述公钥其中之一来至少验证针对所述直接通信的请求,以及

[0267] 所述节点在所述多个UE中的各UE登记至所述节点时从所述多个UE中的各UE接收所述公钥中的各公钥,并且向所述多个UE中的各UE发送不同UE的公钥作为针对成功登记的应答。

[0268] 附注29

[0269] 根据附注28所述的通信系统,其中,还包括服务器,所述服务器用于管理所述公钥,

[0270] 其中,所述节点将所述多个UE中的各UE的所述公钥各自登记至所述服务器,并且从所述服务器获取所述不同UE的公钥,以及

[0271] 所述服务器存储所述节点所登记的公钥,并且通过将所存储的公钥发送至所述节点来应答来自所述节点的请求。

[0272] 附注30

[0273] 一种用于控制UE中的操作的方法,所述方法包括以下步骤:

[0274] 在所述UE成功地登记至节点时登记所述UE的公钥,并且检索一个或多个不同UE的公钥,其中在所述不同UE与所述UE邻近的情况下允许所述不同UE与所述UE进行直接通信,所述节点支持所述直接通信;以及

[0275] 通过使用所述不同UE中的第一UE的公钥来验证来自所述第一UE的用以与所述UE进行直接通信的请求,其中所述请求是由所述第一UE的私钥所保护的。

[0276] 附注31

[0277] 一种用于控制UE中的操作的方法,所述方法包括以下步骤:

[0278] 在所述UE成功地登记至节点时登记所述UE的公钥,并且检索一个或多个不同UE的公钥,其中在所述不同UE与所述UE邻近的情况下允许所述不同UE与所述UE进行直接通信,所述节点支持所述直接通信;以及

[0279] 通过使用所述不同UE中的第一UE的公钥来验证针对用于请求所述第一UE与所述UE进行一对一直接通信的受保护的请求的应答,其中所述应答是由所述第一UE的私钥所保护的。

[0280] 附注32

[0281] 一种节点的控制方法,所述节点支持彼此邻近的允许彼此进行通信的多个UE之间的直接通信,所述控制方法包括以下步骤:

[0282] 在所述多个UE中的一个UE成功地登记至所述节点时,从所述多个UE中的所述一个UE接收公钥;以及

[0283] 向所述多个UE中的所述一个UE发送其它UE的公钥作为针对成功登记的应答,

[0284] 其中,所述多个UE中的各UE使用所述公钥来至少验证针对所述直接通信的请求。

[0285] 附注33

[0286] 一种用于控制服务器中的操作的方法,所述方法包括以下步骤:

[0287] 存储多个UE的公钥,其中在所述多个UE彼此邻近的情况下允许所述多个UE彼此进行直接通信,所述公钥通过支持所述直接通信的节点来进行登记;以及

[0288] 通过将所存储的公钥发送至所述节点来应答来自所述节点的请求,

[0289] 其中,所述多个UE中的各UE使用所述公钥来至少验证针对所述直接通信的请求。

[0290] 本申请基于并要求2013年10月30日提交的日本专利申请2013-225200和2013年10月31日提交的日本专利申请2013-226681的优先权,这两者的全部内容通过引用包含于此。

[0291] 附图标记说明

[0292] 10,10_1-10_m,110,110_1-110_m UE

[0293] 11,21,124 获取单元

[0294] 12 得出单元

[0295] 20,20_1-20_n,120,120_1-120_n ProSe功能体

[0296] 22 分发单元

[0297] 23 指示单元

[0298] 30,130 E-UTRAN

[0299] 40,140 EPC

[0300] 50,150 ProSe APP服务器

[0301] 60,160 第三方(服务器)

[0302] 61,161 存储单元

[0303] 62,162 应答单元

[0304] 111 登记/检索单元

[0305] 112 验证单元

[0306] 121 接收单元

[0307] 122 发送单元

[0308] 123 登记单元

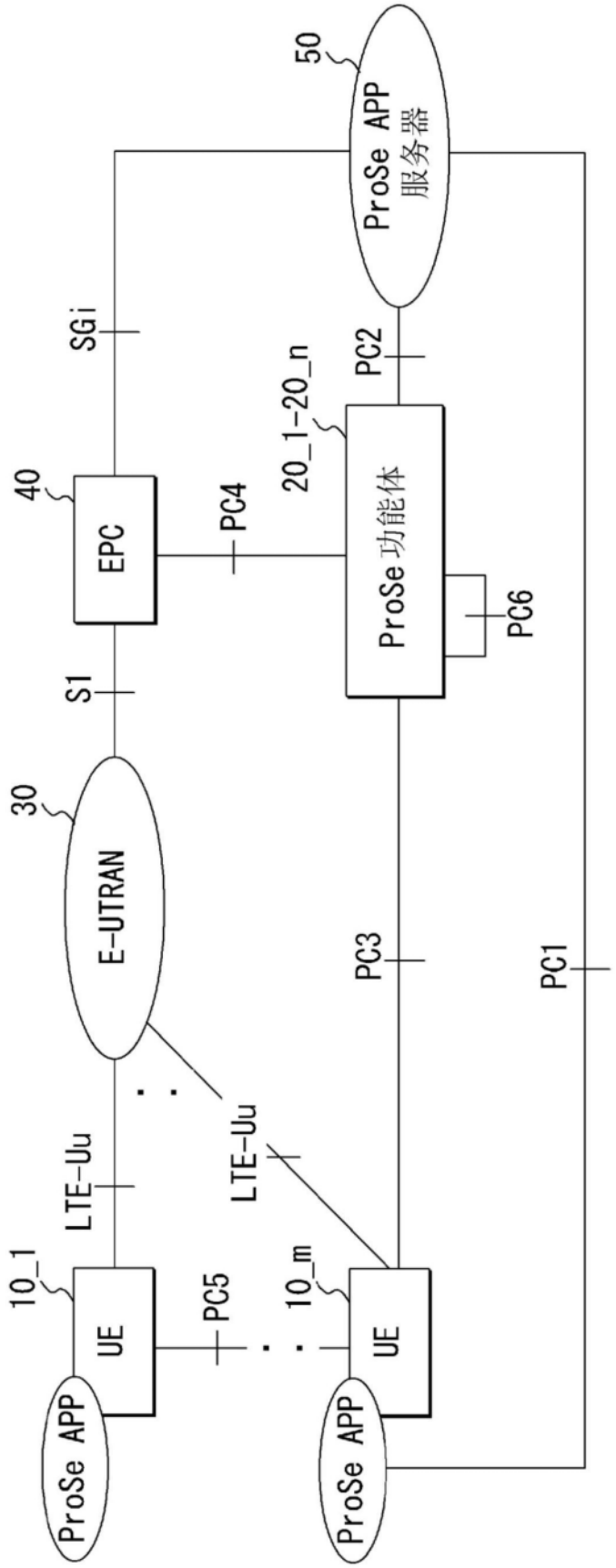

50
ProSe APP
服务器
SGi
PC2
20_1-20_n
ProSe功能体
40
EPC
PC4
PC6
S1
30
E-UTRAN
PC3
PC1
LTE-Uu
LTE-Uu
10_1
UE
PC5
10_m
UE
ProSe APP
ProSe APP

图1

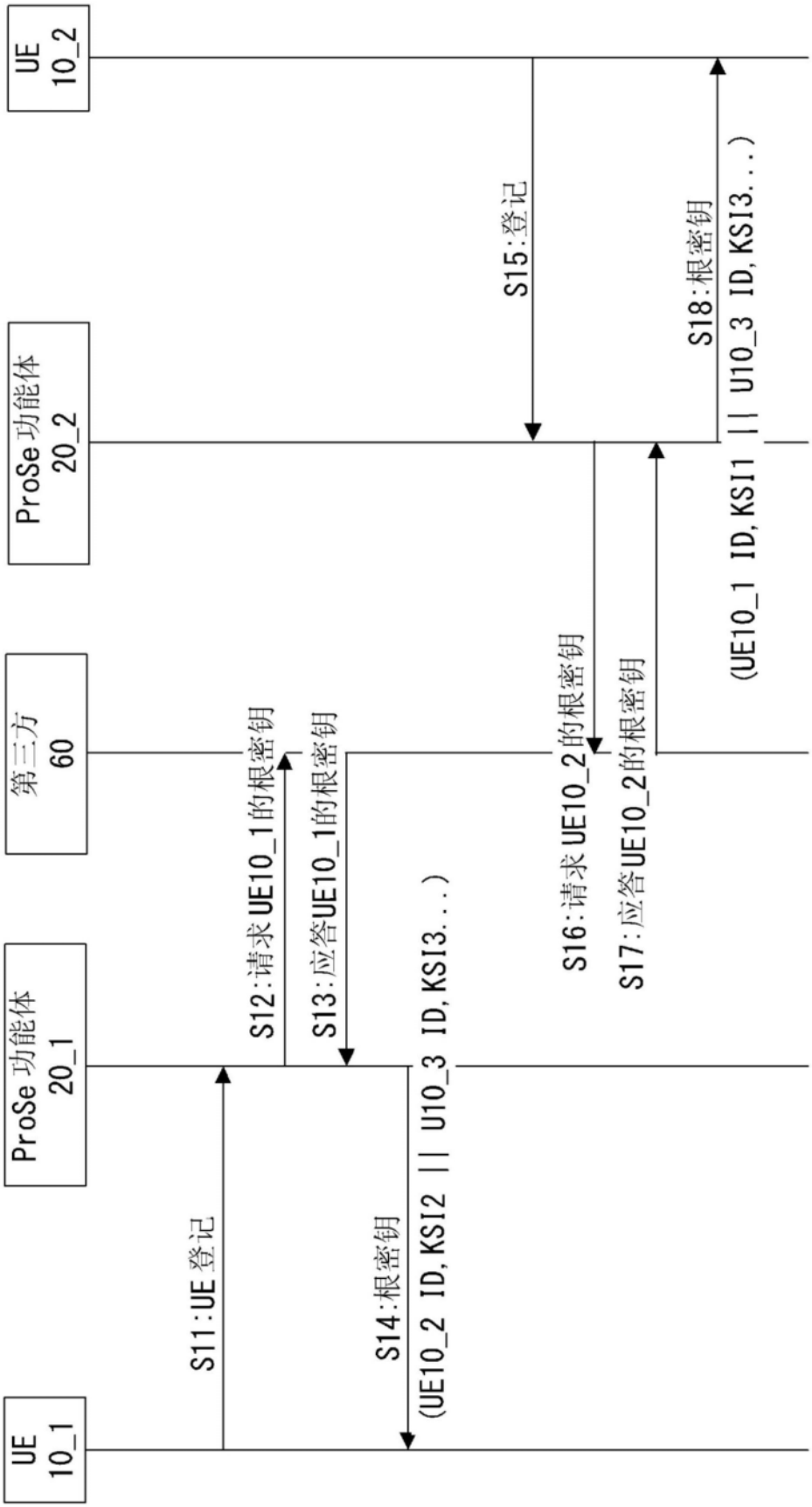

UE 10_2
ProSe 功能体 20_2
第三方 60
ProSe 功能体 20_1
UE 10_1
S11:UE 登记
S12:请求UE10_1的根密钥
S13:应答UE10_1的根密钥
S14:根密钥 (UE10_2 ID,KSI2 || U10_3 ID,KSI3...)
S15:登记
S16:请求UE10_2的根密钥
S17:应答UE10_2的根密钥
S18:根密钥 (UE10_1 ID,KSI1 || U10_3 ID,KSI3...)

图2

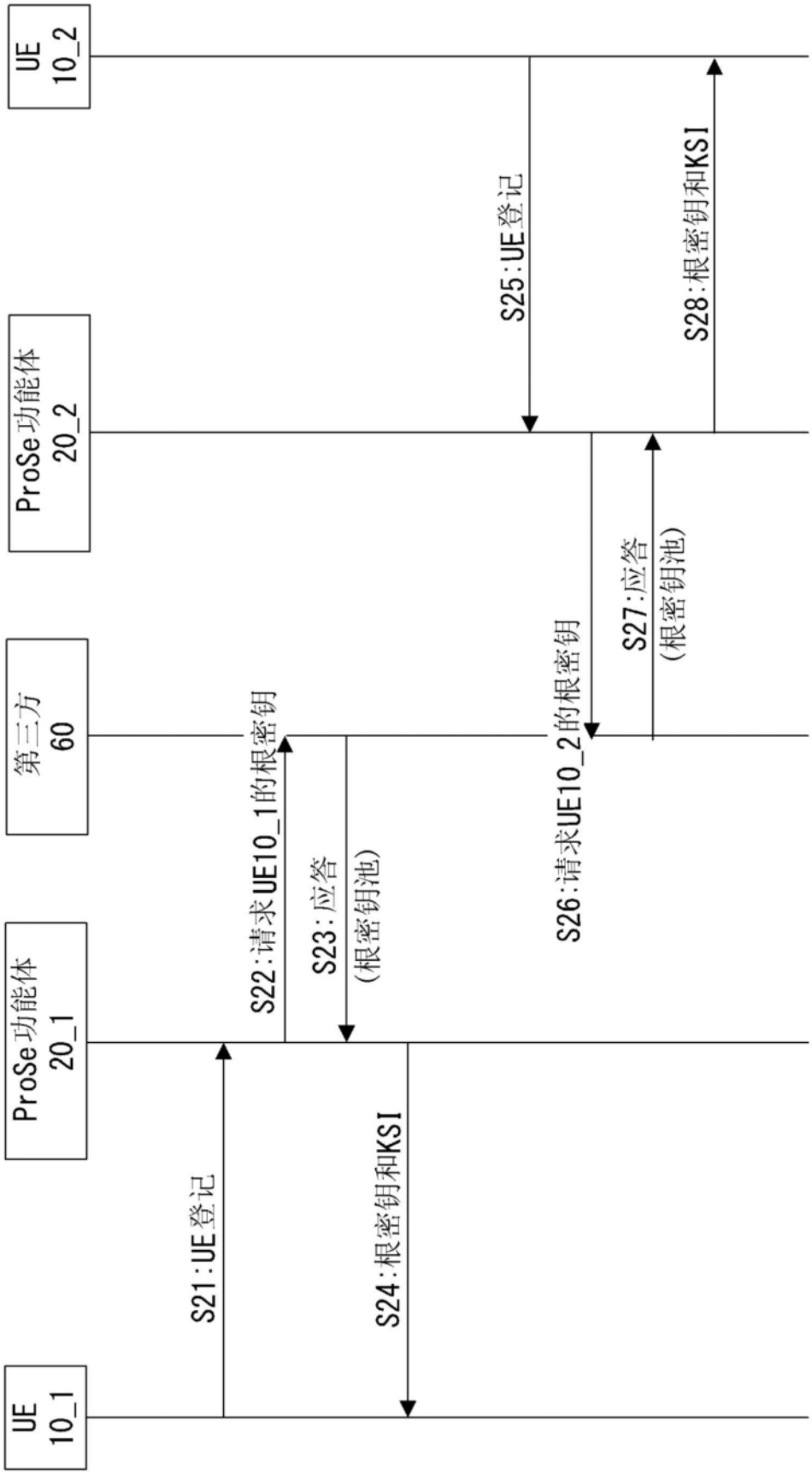

UE 10_1
ProSe功能体 20_1
第三方 60
ProSe功能体 20_2
UE 10_2
S21:UE登记
S22:请求UE10_1的根密钥
S23:应答 (根密钥池)
S24:根密钥和KSI
S25:UE登记
S26:请求UE10_2的根密钥
S27:应答 (根密钥池)
S28:根密钥和KSI

图3

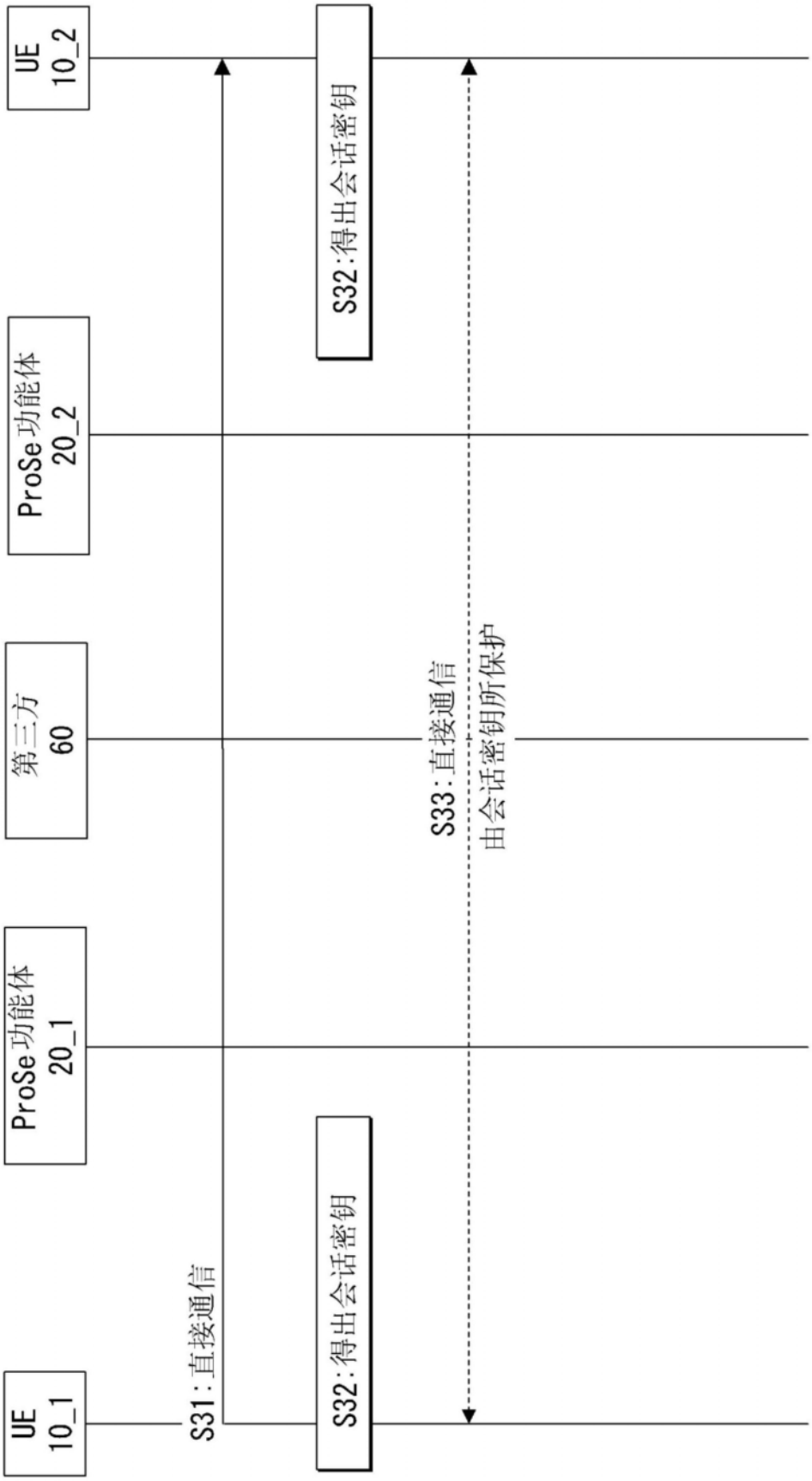

UE 10_2
ProSe功能体 20_2
第三方 60
ProSe功能体 20_1
UE 10_1
S32:得出会话密钥
S33:直接通信
由会话密钥所保护
S31:直接通信
S32:得出会话密钥

图4

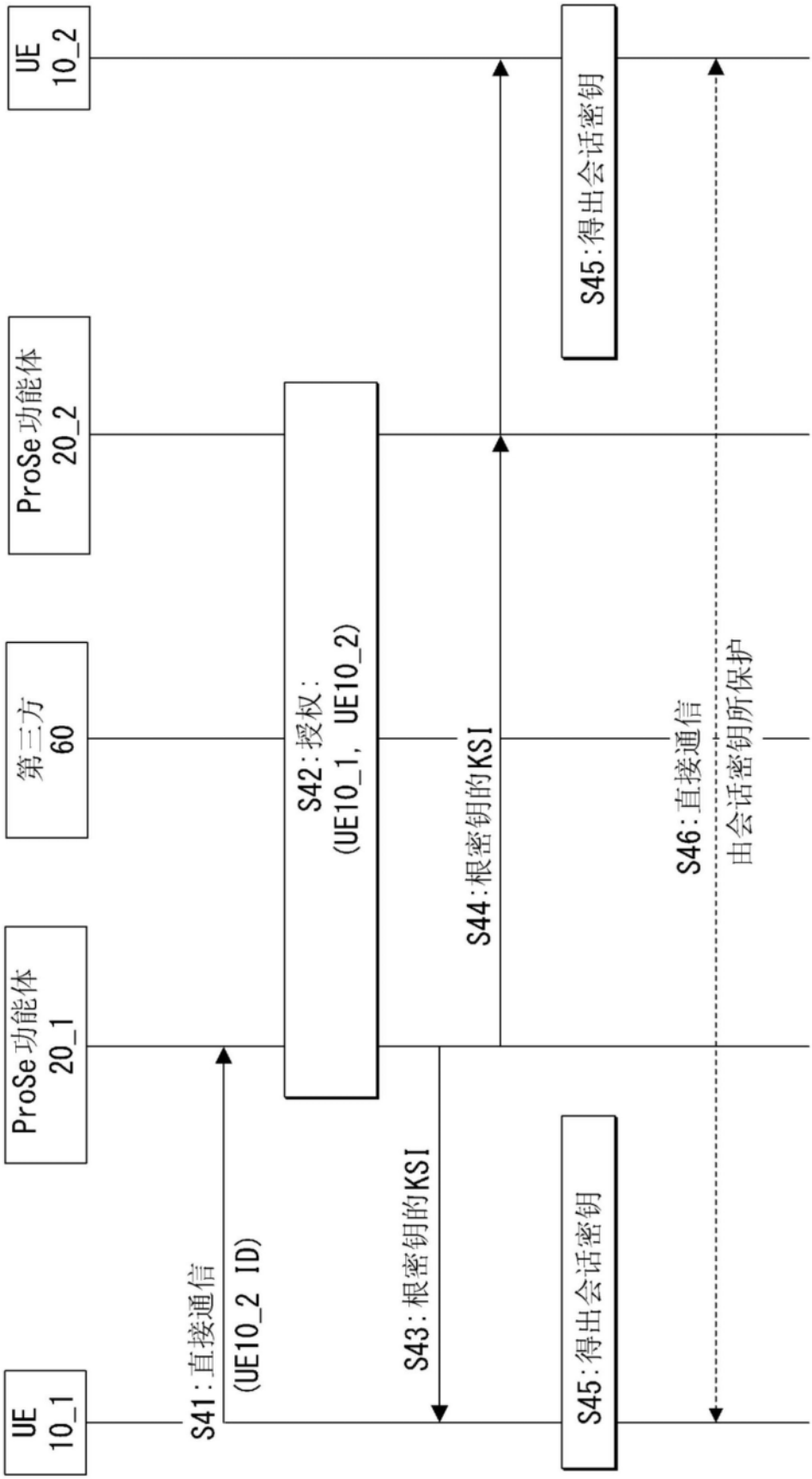

UE 10_1
ProSe功能体 20_1
第三方 60
ProSe功能体 20_2
UE 10_2
S41:直接通信 (UE10_2 ID)
S42:授权: (UE10_1, UE10_2)
S43:根密钥的KSI
S44:根密钥的KSI
S45:得出会话密钥
S45:得出会话密钥
S46:直接通信 由会话密钥所保护

图5

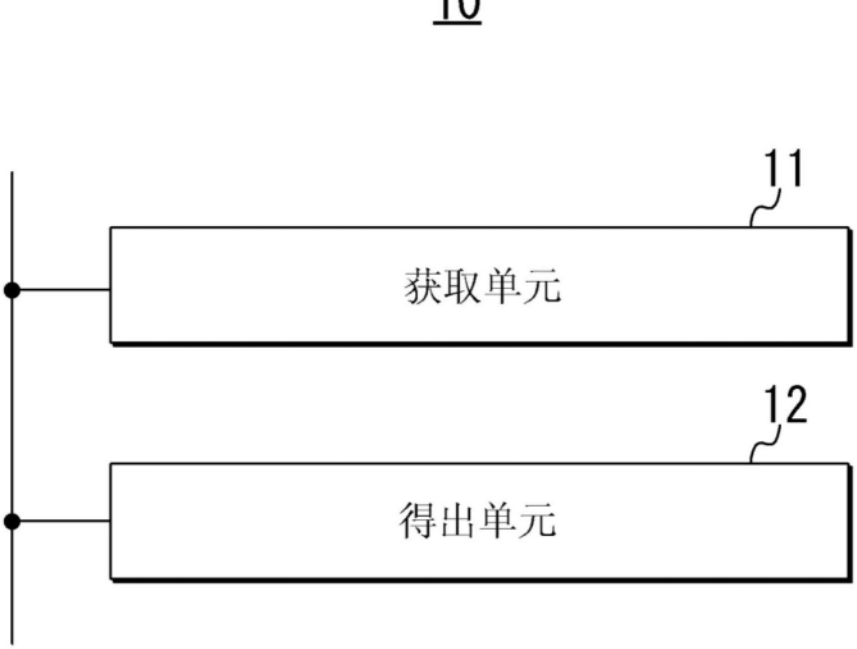


图6

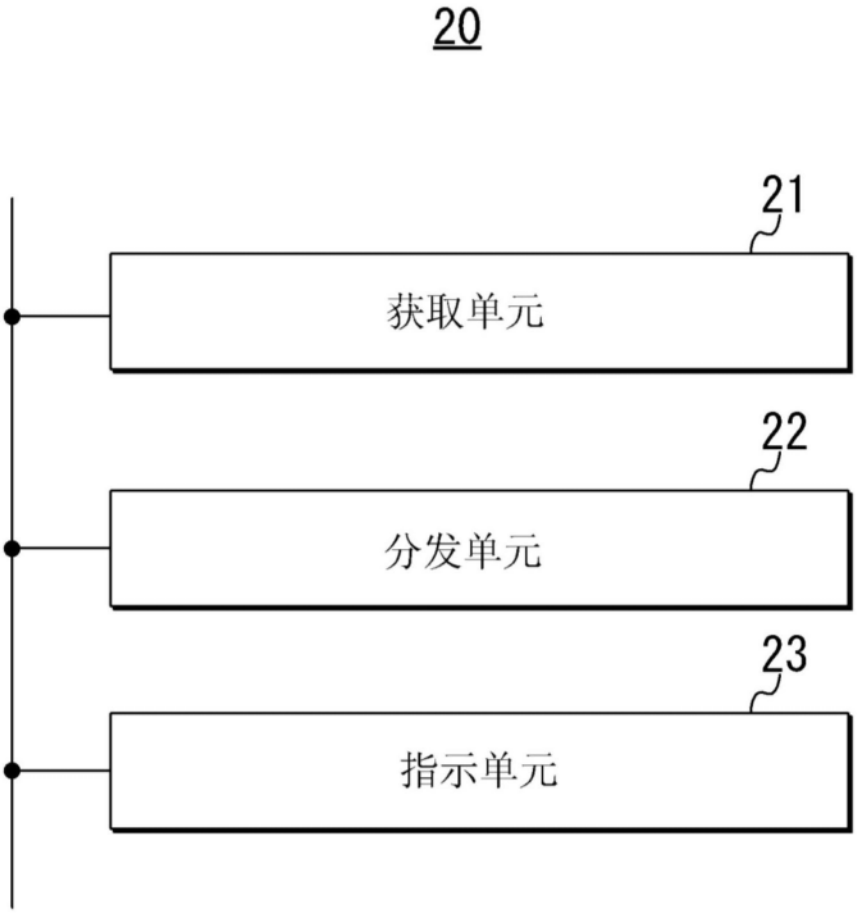


图7

图8

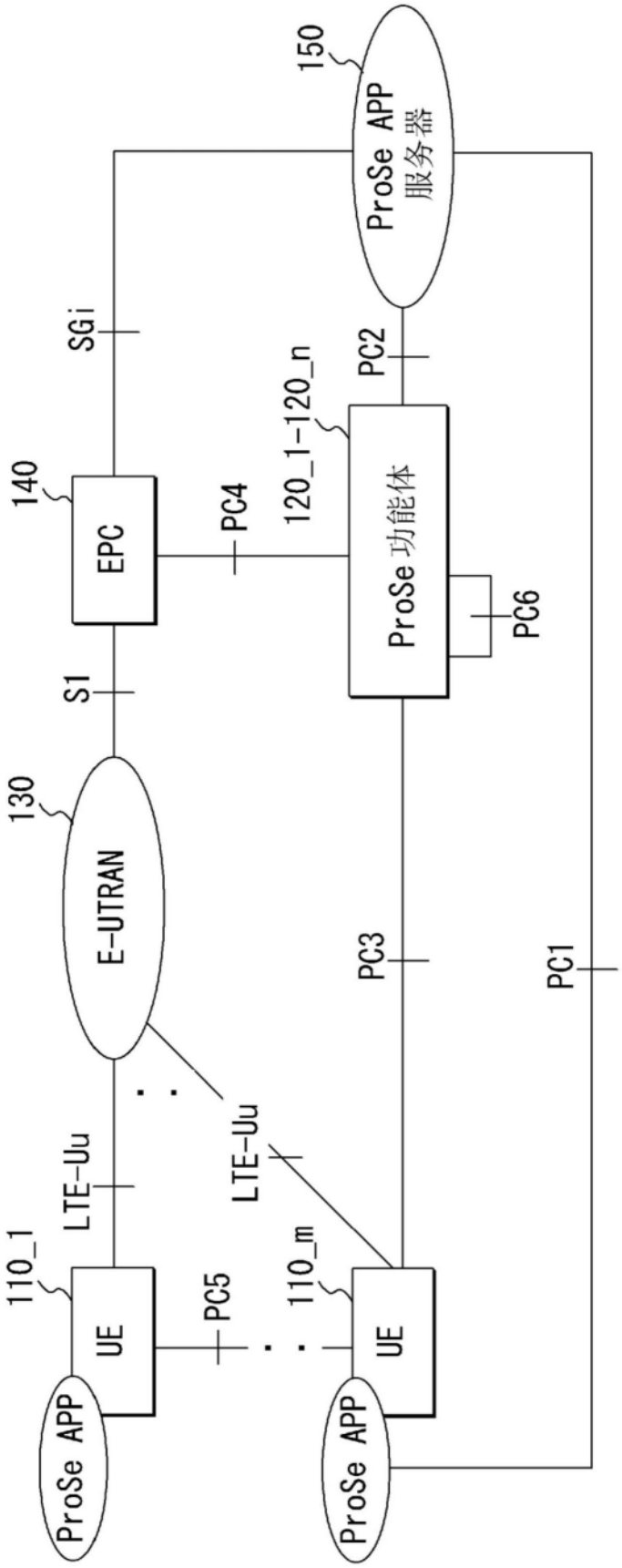

150
ProSe APP
服务器
SGi
PC2
120_1-120_n
140
EPC
PC4
ProSe功能体
PC6
S1
130
E-UTRAN
PC3
PC1
LTE-Uu
LTE-Uu
110_1
110_m
PC5
UE
UE
ProSe APP
ProSe APP

图9

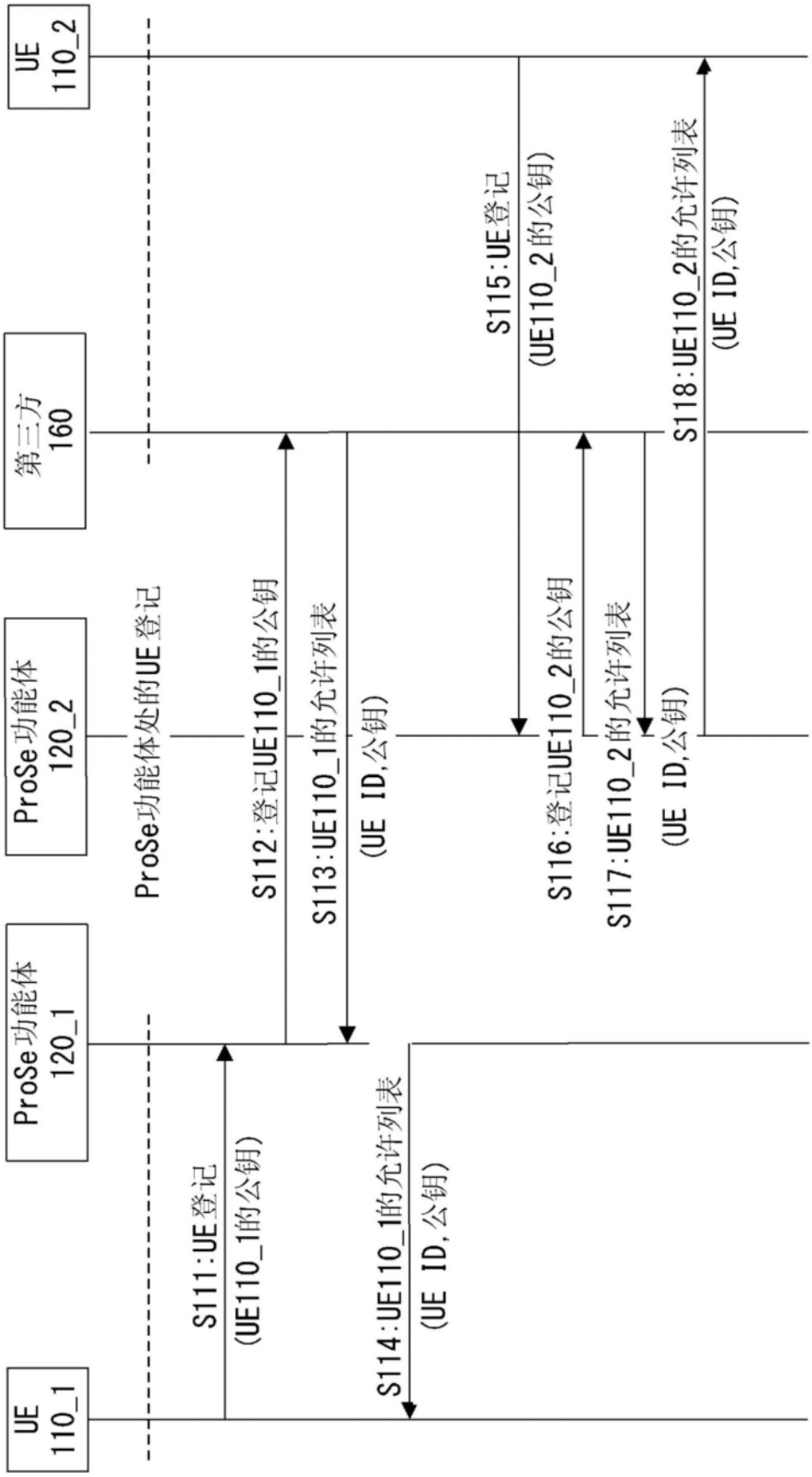

UE 110_1
ProSe功能体 120_1
ProSe功能体 120_2
第三方 160
UE 110_2
ProSe功能体处的UE登记
S111:UE登记 (UE110_1的公钥)
S112:登记UE110_1的公钥
S113:UE110_1的允许列表 (UE ID,公钥)
S114:UE110_1的允许列表 (UE ID,公钥)
S115:UE登记 (UE110_2的公钥)
S116:登记UE110_2的公钥
S117:UE110_2的允许列表 (UE ID,公钥)
S118:UE110_2的允许列表 (UE ID,公钥)

图10

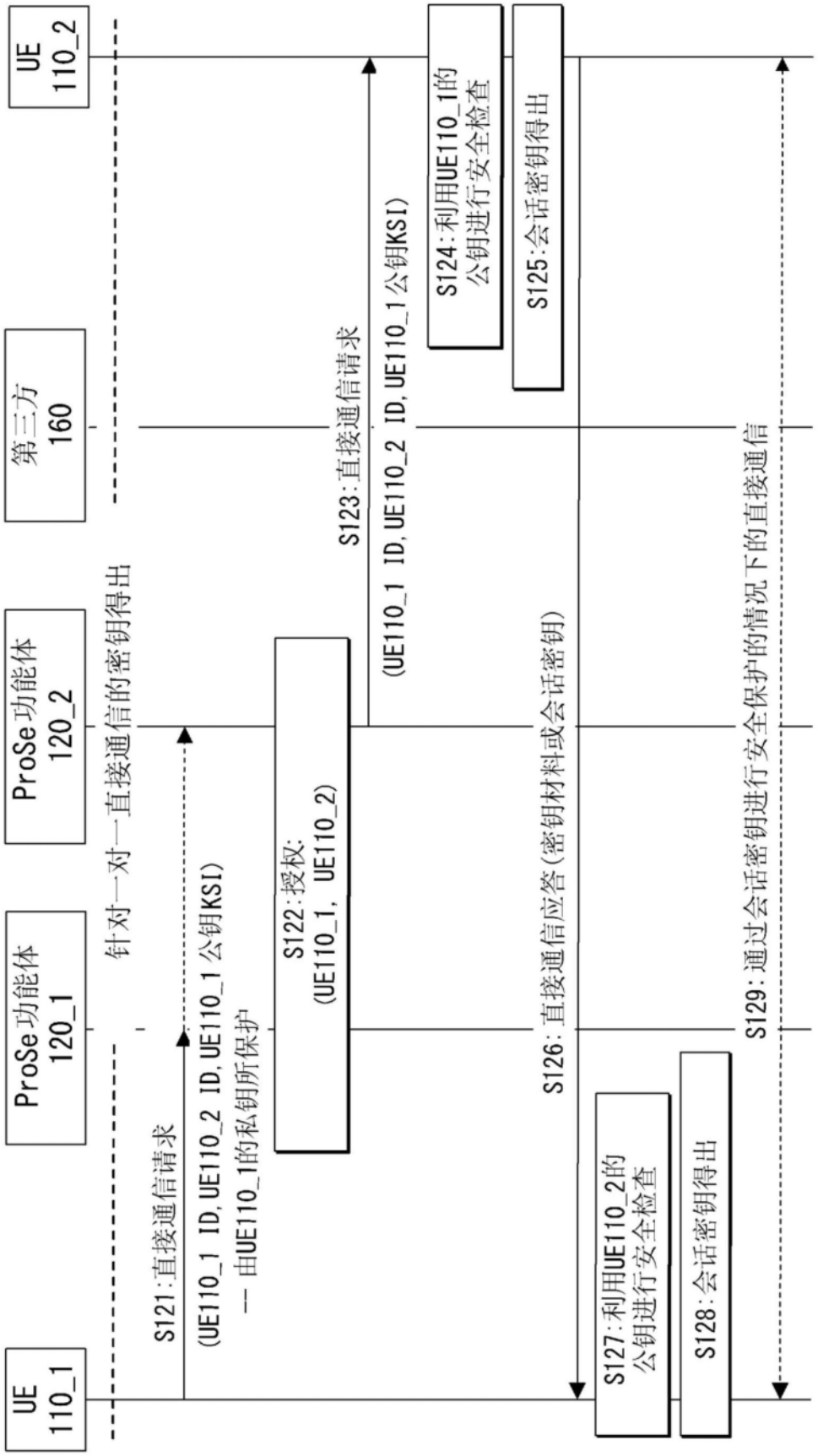

UE 110_1
ProSe功能体 120_1
ProSe功能体 120_2
第三方 160
UE 110_2
针对一对一直接通信的密钥得出
S121:直接通信请求
(UE110_1 ID, UE110_2 ID, UE110_1 公钥KSI)
由UE110_1的私钥所保护
S122:授权:
(UE110_1, UE110_2)
S123:直接通信请求
(UE110_1 ID, UE110_2 ID, UE110_1 公钥KSI)
S124:利用UE110_1的公钥进行安全检查
S125:会话密钥得出
S126:直接通信应答(密钥材料或会话密钥)
S127:利用UE110_2的公钥进行安全检查
S128:会话密钥得出
S129:通过会话密钥进行安全保护的情况下的直接通信

图11

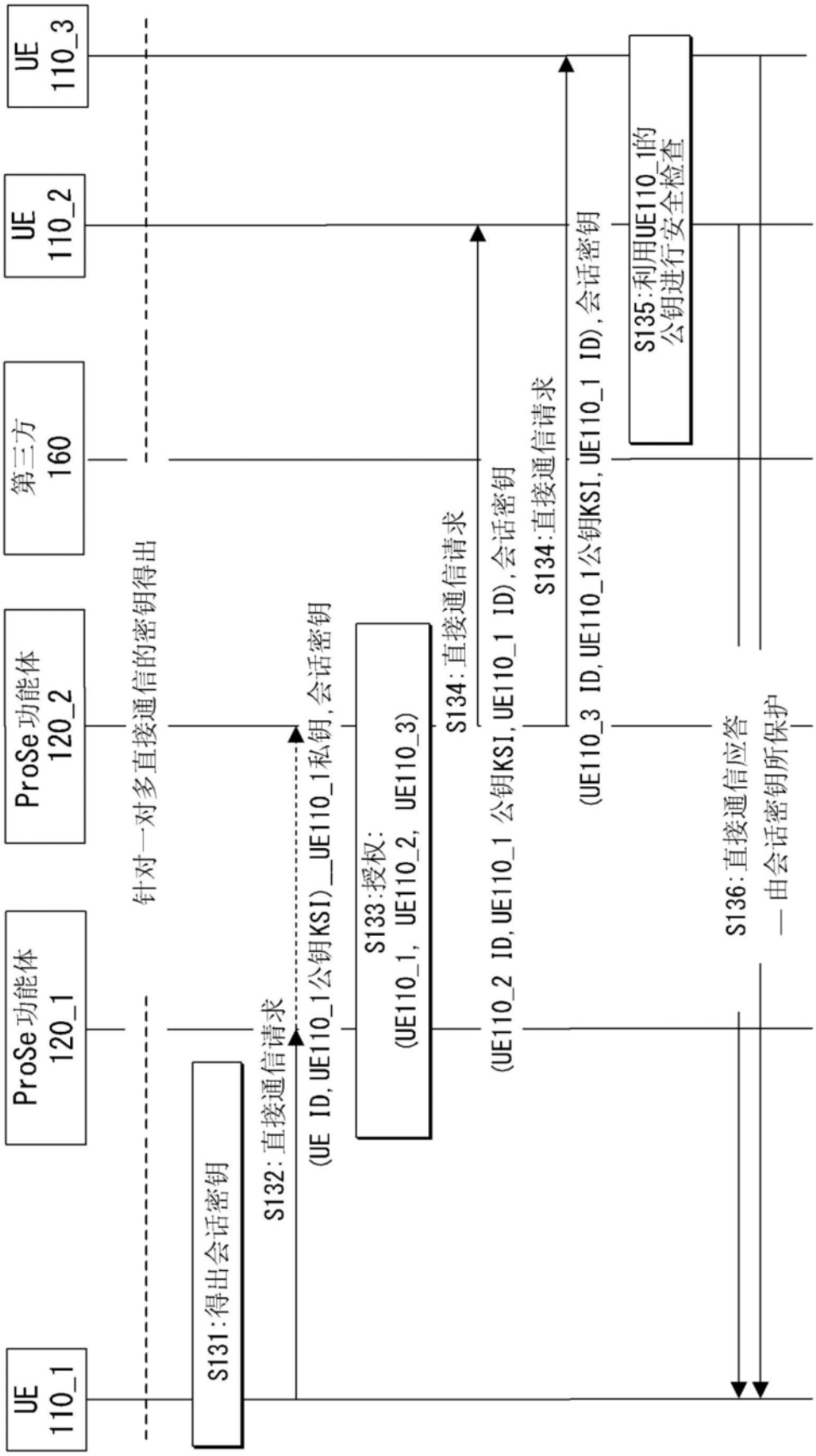

UE 110_1
ProSe功能体 120_1
ProSe功能体 120_2
第三方 160
UE 110_2
UE 110_3
针对一对多直接通信的密钥得出
S131:得出会话密钥
S132:直接通信请求
(UE ID,UE110_1公钥KSI)__UE110_1私钥,会话密钥
S133:授权:
(UE110_1, UE110_2, UE110_3)
S134:直接通信请求
(UE110_2 ID,UE110_1 公钥KSI,UE110_1 ID),会话密钥
S134:直接通信请求
(UE110_3 ID,UE110_1公钥KSI,UE110_1 ID),会话密钥
S135:利用UE110_1的
公钥进行安全检查
S136:直接通信应答
— 由会话密钥所保护

图12


110
111
登记/检索单元
112
验证单元

图13

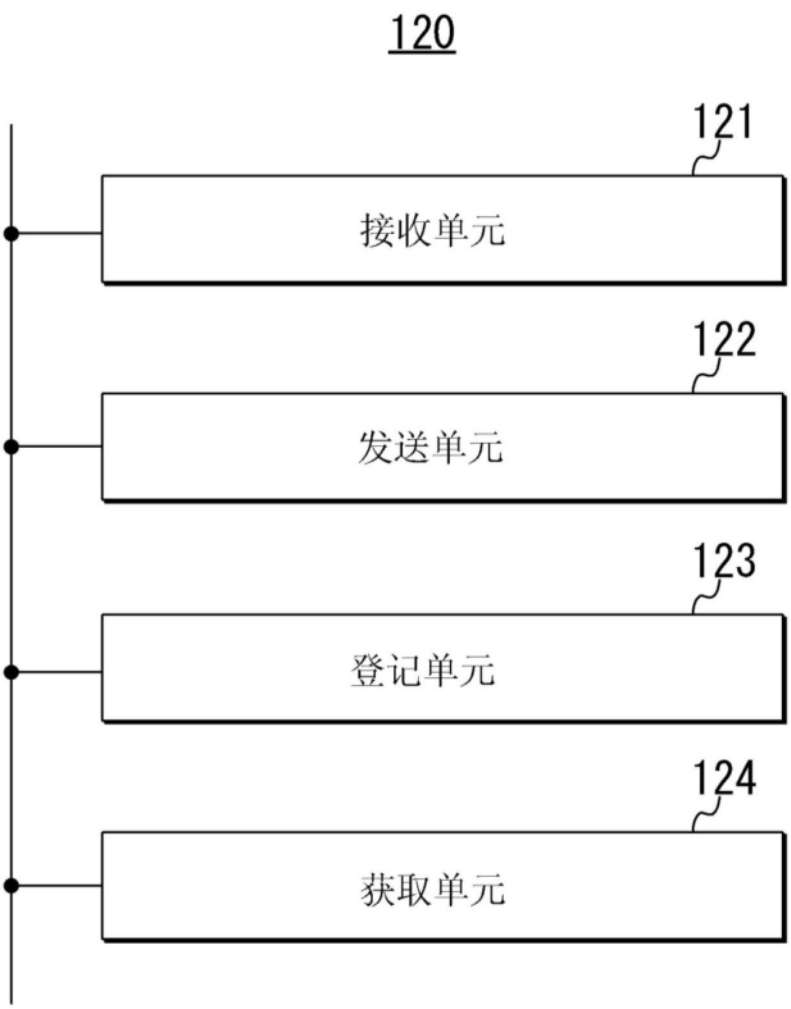

120
121
接收单元
122
发送单元
123
登记单元
124
获取单元

图14

图15