(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 108702353 B
(45)授权公告日 2021.07.27

(21)申请号 201680081592.1
(22)申请日 2016.12.20
(65)同一申请的已公布的文献号
申请公布号 CN 108702353 A
(43)申请公布日 2018.10.23
(30)优先权数据
1562996 2015.12.21 FR
(85)PCT国际申请进入国家阶段日
2018.08.10
(86)PCT国际申请的申请数据
PCT/FR2016/053581 2016.12.20
(87)PCT国际申请的公布数据
WO2017/109389 FR 2017.06.29
(73)专利权人 艾德米亚法国
地址 法国科隆市
(72)发明人 让-菲利普·瓦利尔斯
弗洛里安·加尔多
埃马纽埃尔勒·多塔克斯
弗兰克·隆德皮埃尔
米歇尔·萨托里
(74)专利代理机构 北京康信知识产权代理有限责任公司 11240
代理人 梁丽超 田喜庆
(51)Int.Cl.
H04L 29/06(2006.01)
(56)对比文件
CN 103460738 A,2013.12.18
CN 101859358 A,2010.10.13
CN 1883156 A,2006.12.20
WO 2008150238 A1,2008.12.11
CN 104903907 A,2015.09.09
审查员 李昕萌

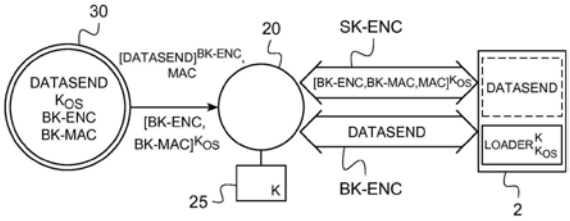
权利要求书1页 说明书10页 附图4页

(54)发明名称

接收电子实体内的数据的方法及相关联的电子实体

(57)摘要

一种用于接收电子实体(2)内的数据(DATASEND)的方法包括下列步骤:在电子实体(2)与外部电子设备之间通过第一密钥(SK-ENC)的加密术来建立第一安全信道;经由第一安全信道接收第一命令;经由第一安全信道接收至少一个第二密钥(BK-ENC);由于执行所述命令,通过第二密钥(BK-ENC)的加密术来创建第二安全信道;在第二安全信道中接收所述数据(DATASEND)。还描述了一种对应的电子实体。



CN 108702353 B

1.一种用于接收电子实体内的数据的方法,其特征在于,所述方法包括以下步骤:

在所述电子实体与外部电子设备之间建立通过会话加密或解密钥匙的加密术而保护的第一安全信道;

经由第一安全信道接收第一命令;

经由所述第一安全信道接收至少一个广播加密或解密钥匙;

将包括所述会话加密或解密钥匙的所述第一安全信道的恢复数据保存在所述电子实体的存储器中;

创建通过所述广播加密或解密钥匙的加密术而保护的第二安全信道作为执行所述第一命令的结果;

接收在第二安全信道中的所述数据;

接收第二命令;

在接收所述第二命令之后,改变至所述第一安全信道,其中,改变步骤包括读取保存在所述存储器中的所述会话加密或解密钥匙的子步骤;以及

在改变步骤之后的使所述恢复数据无效的步骤。

2.根据权利要求1所述的方法,包括:在改变步骤之后的等待所述第一安全信道中的授权命令的步骤。

3.根据权利要求2所述的方法,包括检查所述第一安全信道中的完整性验证码的步骤。

4.根据权利要求1至3中任一项所述的方法,其中,所述会话加密或解密钥匙是从储存在所述电子实体中的静态钥匙得出的会话钥匙。

5.根据权利要求1至3中任一项所述的方法,其中,所述广播加密或解密钥匙是用于对由另一电子实体建立的安全信道进行加密的广播钥匙。

6.根据权利要求1至3中任一项所述的方法,其中,所述数据表示所述电子实体的操作系统的一部分或表示所述电子实体稍后能够使用的应用程序或数据的至少一部分。

7.根据权利要求1至3中任一项所述的方法,其中,所接收的数据储存在所述电子实体的非易失性存储器内。

8.根据权利要求1至3中任一项所述的方法,其中,所述电子实体是安全元件。

9.根据权利要求1至3中任一项所述的方法,其中,所述外部电子设备是移动终端或供能仪表或连接的对象或便携式对象。

10.一种电子实体,其特征在于,包括:

用于在所述电子实体与外部电子设备之间建立通过会话加密或解密钥匙的加密术而保护的第一安全信道的模块;

用于经由第一安全信道接收第一命令和广播加密或解密钥匙的模块;

用于存储包括所述会话加密或解密钥匙的所述第一安全信道的恢复数据的存储器;

用于将通过所述广播加密或解密钥匙的加密术而保护的第二安全信道创建为执行所述第一命令的结果的模块;

用于在第二安全信道中接收数据和第二命令的模块;

用于在接收所述第二命令之后改变至所述第一安全信道的模块,包括用于读取保存在所述存储器中的所述会话加密或解密钥匙的单元;以及

用于在改变至所述第一安全信道之后的使所述恢复数据无效的模块。

接收电子实体内的数据的方法及相关联的电子实体

技术领域

[0001] 本发明涉及电子装置之间的数据的安全交换。

[0002] 更具体地，本发明涉及一种用于接收电子实体内的数据的方法并且涉及一种相关联的电子实体。

[0003] 本发明特别有利地应用于必须将相同的数据安全地传送到大量电子实体的情况。

背景技术

[0004] 为了能够在两个电子装置之间保密地交换数据，已知在这两个电子装置之间建立通过密钥的加密术来保护的信道，对于该加密术，存在例如在文献“GlobalPlatform Card Technology-Secure Channel Protocol 03-Card Specification v 2.2Amendment D”(v1.1)中描述的称为“SCP03”的协议中的规定。

[0005] 在该协议的上下文中，为了确保对数据的有效保护，密钥是从仅对两个电子装置已知的静态钥匙推导的会话钥匙。

[0006] 然而，该解决方案不适合于将同一数据集发送到大量电子实体(例如在更新大量安全元件的操作系统的一部分的活动中的情况)的情况，因为其随后有必要为所讨论的每个电子实体准备专用的加密版本。

发明内容

[0007] 在该上下文中，本发明提出了一种用于在电子实体内接收数据的方法，其特征在于包括以下步骤：

[0008] 在电子实体与外部电子设备之间建立通过第一密钥的加密术而保护的第一信道；

[0009] 经由第一安全信道接收第一命令；

[0010] 经由第一安全信道接收至少一个第二密钥；

[0011] 创建通过第二密钥的加密术而保护的第二信道作为执行所述第一命令的结果；

[0012] 在第二安全信道中接收所述数据。

[0013] 如上所述，因此，第一安全信道可以是多样化的，以使用例如SCP03类型的协议将第二密钥安全地传送至电子实体。

[0014] 然而，创建第二安全信道能够随后使用不同加密术，该加密术是在需要时基于用于加密旨在用于大量电子实体的数据的第二密钥。

[0015] 例如，第一安全信道基于在非预测模式下的SCP03类型的协议，但是例如，第二安全信道基于在预测模式下的SCP03类型的协议。

[0016] 例如，第二密钥包括在第一命令中。

[0017] 可选地考虑的其他特征如下：

[0018] 该方法包括在接收所述第一命令的步骤之后并且在创建第二安全信道的步骤之前的将第一密钥(并且例如，还有相关联的上下文数据)保存在电子实体(第一密钥及形成第一安全信道的恢复数据的可能的相关联上下文数据)的存储器(例如，随机访问存储器)

中的步骤；

[0019] 在接收所述数据与第二命令的步骤之后，该方法包括改变成第一安全信道的步骤；

[0020] 改变步骤包括读取(随机访问)保存在存储器中的第一密钥的子步骤；

[0021] 在改变步骤之后，该方法包括使第一安全信道的恢复数据无效的步骤；

[0022] 在改变步骤之后，该方法包括在第一安全信道中等待授权命令的步骤；

[0023] 在改变步骤之后，该方法可以包括在第一安全信道中接收完整性验证码的步骤：

[0024] 第一密钥是从存储在电子实体中的静态钥匙推导的会话钥匙；

[0025] 第二密钥是用于加密由另一电子实体建立的安全信道的广播钥匙；

[0026] 例如，数据表示操作系统的一部分、电子实体稍后能够使用的应用程序或其他数据的至少一部分；

[0027] 所接收的数据存储在电子实体的非易失性存储器中；

[0028] 电子实体是安全元件；

[0029] 外部电子设备是移动终端或供能仪表或连接的对象或便携式对象。

[0030] 本发明还提出了一种电子实体，其特征在于，包括：用于在电子实体与外部电子设备之间建立通过第一密钥的加密术而保护的第一信道的模块；用于经由第一安全信道接收第一命令和第二密钥的模块；用于将通过第二密钥的加密术而保护的第二信道创建为执行所述第一命令的结果的模块；以及用于在第二安全信道中接收数据的模块。

[0031] 当电子实体包括处理器时，至少一些模块可以至少部分地通过存储在电子实体的存储器中的计算机程序指令来实现，并且可被设计成当通过处理器执行这些指令时，至少一些模块有助于实现所讨论的模块的功能。

[0032] 具体地，刚刚被提出的解决方案具有下列优点：

[0033] 可以根据电子元件的运营商、制造商或其他供应商的要求调整安全级别(通过多样化或非多样化信道以及还有安全元件(例如，MAC)发送的数据的选择)，从而使安全级别变得灵活；

[0034] 允许在终端上的延迟部署。通过广播模式发送数据并且可以稍后发送授权命令，以触发加载数据的使用。通过该授权命令，(供应商或制造商的)服务器仍保持对安全元件的控制(由于在授权之前，存在执行的完整性监测阶段)。使用该命令的多样化信道使得可以单独寻址终端并且确保在期望的时间内执行操作并且具有期望的效果。

[0035] 保存上下文的规定(进一步参见步骤E18)使得在从一种模式改变成另一模式时不可以重启多样化模式的配置。

[0036] 具体地，在下列实施例中，存在用于保存多样化模式的上下文的规定。在其他实施方式中，仍然可以在改变成另一种模式之前为所使用的每种模式保存的下文(例如，多样化和多用户)。

附图说明

[0037] 将通过非限制性实施例给出的、参考附图的下列描述给出关于本发明的构成以及如何能够实现本发明的更好理解。

[0038] 在附图中：

[0039] 图1示出了本发明的上下文中使用的示例性安全元件；

[0040] 图2是示出在图1的安全元件内实现的示例性方法的流程图；

[0041] 图3示出了使用图2中的方法的第一可能上下文；

[0042] 图4示出了使用图2中的方法的第二可能上下文；并且

[0043] 图5是示出用于更新图1的安全元件的操作系统的示例性方法的流程图。

具体实施方式

[0044] 图1示出了本发明的上下文中使用的示例性安全元件2。

[0045] 例如，通过微控制器的形式实现该安全元件2(或SE)。这样的安全元件2可以被集成到电子设备中，例如，被焊接在电子设备内部：那么，安全元件属于eSE(用于“嵌入式安全元件”)类型。

[0046] 作为变型，安全元件2可以是微电路卡(例如，通用微电路卡或用于“通用集成电路卡”UICC)、或焊接通用微电路卡、或用于“嵌入式通用电路卡”的eUICC。

[0047] 安全元件2包括处理器4(例如，微处理器)、非易失性存储器6(例如，可重写的非易失性存储器)、以及随机访问存储器8。

[0048] 例如，非易失性存储器6属于Flash或NVRAM类型。

[0049] 非易失性存储器6存储程序指令，在通过处理器4执行这些指令时，该程序指令使安全元件2实现数据处理方法(具体地，下面参考图2描述的方法)。

[0050] 非易失性存储器6还存储实现该方法时使用的数据：非易失性存储器6具体存储下面描述的方法中使用的密钥(被称为静态钥匙)，具体是一组静态密钥K。

[0051] 随机访问存储器8存储通过在安全元件2内实现的方法操纵的数据。

[0052] 安全元件2还包括能够使处理器4与其他电子装置交换数据的至少一个接口10。当安全元件2是微控制器时，接口10可以由微控制器的一个或多个管脚形成。如果安全元件是微电路卡，接口则包括暴露在微电路卡的上面上的至少一个触点。接口还可以是ISO、SWP、或其他SPI类型的端口。

[0053] 图2示出了在安全元件2内实现的示例性方法。

[0054] 该方法开始于步骤E2，由处理器4和接口10接收包含主机口令HCH的启动命令IU。

[0055] 出于与安全元件2交换安全数据之目的，之前已经通过期望建立安全通信信道的电子设备(与安全元件2分离)发送了该启动命令IU以及由如下所述的安全元件2接收的其他命令。

[0056] 例如，如在文献“GlobalPlatform Card Technology-Secure Channel Protocol 03-Card Specification v 2.2Amendment D”的第7.1.1段所定义的或者在文献“GlobalPlatform Card Specification v 2.2”的附件D.4.1中定义的，启动命令IU是INITIALIZE UPDATE类型的命令。

[0057] 在收到启动命令IU时，处理器E4实现(现在描述的)步骤E4和E6。

[0058] 例如，在步骤E4中，处理器4通过随机抽取(random drawing)或作为变型通过伪随机确定来生成卡口令(card challenge)CCH。伪随机确定使得可以通过基于存储在电子实体2内的数据的计算来获得未授权的第三方实体不能够预测的卡口令CCH。然而，授权的第三方的伪随机确定使得可以计算卡口令并且可以预生成卡口令。

[0059] 在这种情况下,例如,使用在文献“GlobalPlatform Card Technology-Secure Channel Protocol 03-Card Specification v 2.2Amendment D”(v1.1)的第6.2.2.1段中定义的卡口令CCH的伪随机确定的实例。在该实施例中,基于发送启动命令IU的应用程序的标识符与存储在非易失性存储器6中的一组静态密钥K中的密钥K-ENC的序列计数器来确定卡口令CCH。

[0060] 在步骤E6中,处理器4随后在这种情况下通过使用存储在非易失性存储器6中的一组静态密钥K中的静态钥匙来生成一组会话钥匙SK。具体地,在该步骤中,处理器4基于已经提及的密钥K-ENC,并且在这种情况下,还基于主机口令HCH和卡口令CCH来生成会话密钥或解密钥匙SK-ENC,例如,根据文献“GlobalPlatform Card Technology-Secure Channel Protocol 03-Card Specification v 2.2Amendment D”(v1.1)的第6.2.1段的规定。

[0061] 然后,安全元件2可以将在步骤E4中生成的卡口令CCH返回至发送命令的电子设备。如在这种情况下描述的,当通过伪随机确定获得卡口令CCH时,因为发送命令的电子设备能使用相同的伪随机确定处理获得卡口令CCH,所以不需要发送卡口令CCH。

[0062] 然后,处理器4在接口10上接收伴随有主机密码HAC的验证命令EA。已经预先通过使用一组会话钥匙的会话钥匙S-MAC、主机口令HCH(如上所述,之前与启动命令IU一起发送)、以及卡口令CCH(如上所述,在这种情况下,通过伪随机确定获得)在发送命令的电子设备内确定该主机密码HAC。

[0063] 例如,如在文献“GlobalPlatform Card Technology-Secure Channel Protocol 03-Card Specification v 2.2Amendment D”(v1.1)的第7.1.2段或文献“GlobalPlatform Card Specification v 2.2”的附件D.4.2中定义的,启动命令EA是EXTERNAL AUTHENTICATE类型的命令。

[0064] 然后,在步骤E10中,处理器验证所接收的主机密码HAC实际是否对应于期望的密码,由此使得可以验证发送命令的电子设备。

[0065] 如果否,则该方法继续至步骤E12,其中,处理器4结束交换,而不建立安全信道。

[0066] 相反,如果所接收的主机密码HAC实际上对应于期望的密码,则在发送命令的电子设备与安全元件2之间建立安全信道。由于用于确保交换的保密性的会话钥匙SK(具体地,会话加密或解密钥匙SK-ENC)仅对于发送命令的电子设备和安全元件2是已知(并且例如,如果发送命令的电子设备期望与另一安全元件建立安全信道,则将会不同),因此该安全信道被视为是多样化的(参见图2中的参考DIVERSIF)。

[0067] 应注意,在SCP-03协议的情况下,使用通用名称为SK-ENC、SK-MAC、以及SK-RMAC等三个多样化的密钥。

[0068] 然后,在步骤E14中,处理器4经由该安全信道(并且此外,在此处描述的实施例中,还通过加密计数器并且通过验证码链接值)接收伴随有一组广播钥匙BK的改变命令CHM。在这种情况下,例如,建议引进专用命令(被称为CHANGE MODE)形式的该改变命令。

[0069] 如上所述,由于建立安全信道的事实,通过会话加密或解密钥匙SK-ENC加密附加至命令的数据(具体地,在这种情况下,广播钥匙BK,例如,附加数据使得可以创建第二安全信道)。

[0070] 由此,在步骤E16中,处理器4通过使用会话加密或解密钥匙SK-ENC(如上所述,在步骤E6中获得的)的(在这种情况下为对称的)密码解密算法来解密广播钥匙BK。例如,所使

用的密码算法是AES类型。

[0071] 然后，在步骤E18中，处理器4将上下文(在图2中表示为BCK.UP)保存在随机访问存储器8(或作为变型，非易失性存储器6)的专用区域中。具体地，处理器4将会话钥匙SK(包括会话加密或解密钥匙SK-ENC)保存在随机访问存储器8的该专用区域中。

[0072] 在这种情况下描述的实施例中，其中，安全信道的协议属于SCP03类型，处理器4还将与多样化的安全信道相关联(并且与在步骤E14中接收的这些安全信道分离)的加密计数器和验证码链接值(“MAC链接值”)保存在专用区域中。

[0073] 然后，在步骤E20中，处理器4改变成广播模式或多用户模式(参见图2中的MULTIU.)，其中，使用广播钥匙BK，而非会话钥匙SK。在这种情况下，在该广播模式中，还使用在步骤E14中接收的加密计数器和链接值。

[0074] 具体地，在该广播(或多用户)操作模式中，发送命令的电子设备与安全元件2能够在通过广播加密或解密钥匙BK-ENC(而非使用会话加密或解密钥匙SK-ENC)的加密术来确保其保密性的安全信道中进行交换。

[0075] 如下文中将要说明的，由于使用广播钥匙BK处理(具体地，加密)旨在用于多个(或甚至大量)安全元件的数据的事实，该操作模式被称为“广播”或“多用户”。

[0076] 然后，在步骤E22中，处理器接收附加有数据Di的命令CMDi。如已经指出的，由于在步骤E20中改变成广播模式(或多用户模式)，现通过广播加密或解密钥匙BK-ENC来加密附加至接收命令的数据。

[0077] 由此，在步骤E24中，处理器4通过应用使用在步骤E14中接收的广播加密或解密钥匙BK-ENC的(在这种情况下为对称的)密码解密算法来解密数据Di。

[0078] 由此，在通过保存在非易失性存储器6中的这种情况下，可以在安全元件2内使用解密数据Di(步骤26)。如进一步说明的，在这种情况下，例如，提出数据Di至少表示从远程服务器被加载至安全元件2中的应用操作系统的一部分。然而，作为变型，这些数据可以表示通过位于操作系统的外部的应用程序部件使用的应用程序(不构成操作系统的一部分)、密钥、或数据。

[0079] 作为接收多个命令CMDi(例如，对于N个命令CMDi，如图2中指出的，其中，i＝1...，N)的结果，步骤E22至步骤E26可能被重复。

[0080] 当已经收到在广播模式(或多用户模式)下实现的全部命令时，处理器4出于返回至多样化模式的目的而接收改变命令CHM(步骤E28)，例如，CHANGE MODE类型的上述命令。

[0081] 具体地，在这种情况下，当处理器4以多样化模式操作时，存在能够改变成广播(或多用户)模式的一个及相同命令的规定，并且当处理器4以广播模式操作时，则改变成多样化模式。作为变型，两个单独的命令可以分别被创建为用于实现这两种变化。

[0082] 在收到该命令时，处理器4读取随机访问存储器8的上述的区域中的会话钥匙SK(其中，如上所述，在步骤E18中保存这些会话钥匙)，以及在这种情况下，处理器4读取加密计数器和链接值，并且在步骤E30中，改变成使用这些会话钥匙SK的多样化模式。由此，处理器4可以再次使用由步骤E2至E10创建的安全信道。因此，在到多样化模式的这种改变之后，可能存在使得恢复数据无效(例如，被擦除)的规定，因此，稍后将不可以再次执行该改变。

[0083] 然后，在步骤E32中，处理器4接收授权命令ATHZ，可能在该步骤的若干执行过程中，授权命令ATHZ附加有允许验证在步骤E26中安装(即，存储，在这种情况下，存储在非易

失性存储器6中)的数据Di的完整性验证码MAC。下面给出了获得完整性验证码MAC的实施例。

[0084] 例如,授权命令是在这种情况下提出引进的名为AUTHORIZE_ACTION的新命令。

[0085] 利用形成上述的安全信道中的交换的一部分的授权命令ATHZ,通过会话加密或解密钥匙SK-ENC而加密附加至该命令的数据(在这种情况下,为完整性验证码MAC)。

[0086] 由此,在步骤E34中,处理器4通过应用使用会话加密或解密钥匙SK-ENC的(在这种情况下,为对称的)密码解密算法来解密完整性验证码MAC。在这种情况下,密码算法是AES类型的算法。

[0087] 然后,在步骤E36中,处理器4可以通过使用被解密的完整性验证码MAC来验证在步骤E26的执行过程中存储在非易失性存储器6中的数据Di的完整性。

[0088] 如果步骤E36中的验证失败,处理器4则不使用数据Di,而是例如,通过将错误消息返回至负责生成命令的电子设备(例如,远程服务器)而在步骤E38中实现纠错处理操作。

[0089] 如果步骤E36中的验证成功,则处理器4例如在步骤E40中命令经由接口10发送校正操作消息。然后,在其操作过程中,处理器4将使用在步骤E26中存储在非易失性存储器6中的数据Di。在下文描述的实施例中,将通过处理器4执行由数据Di表示的应用操作系统的至少一些部分。

[0090] 图3和图4示出了使用诸如刚刚描述的方法的两个可能上下文。

[0091] 在这两个上下文中,期望将操作系统或其他应用的应用程序部分DATASEND安全地安装在安全元件2中(即,加载至非易失性存储器6中)。例如,在这种情况下,安全元件2上的主要部分LOADER(即,存储在非易失性存储器6中)负载加载被发送的数据。在一个实施方式中,在不部署主要部分LOADER的情况下(在这种情况下,例如,这是能够执行的单独应用,不被加载之后的主要部分LOADER干扰),安全元件2可以使用被发送的数据。在另一实施方式中,主要部分LOADER还可以用于启动被加载数据的部署。

[0092] 在设计计算机系统30中,应用程序部分DATASEND是可用的。例如,由安全元件2的制造商管理该设计计算机系统30。设计计算机系统30具有高的安全级别。

[0093] 应用程序部分DATASEND必须经由(例如,通过移动电话制造商或运营商管理的)管理服务器20发送至安全元件2。准确地说,安全元件2与该移动电话制造商或运营商相关联。准确地说,安全元件2存储允许承载安全元件2的用户终端访问由移动电话运营商操作的至少一个移动电话网络的数据。

[0094] 为简单起见,图3和图4中未提及上述的用户终端。然而,应当理解的是,管理服务器20与安全元件2之间的数据的交换使用用户终端的电信装置(并且可能还有上述的移动电话网络)。

[0095] 管理服务器20具有中等安全级别。然而,提供了安全模块25,其(经由安全链接)链接至管理服务器20(例如,通过有线链接,在这种情况下为以太网类型)并且其自身具有高安全级别。

[0096] 例如,安全模块25是HSM(用于“硬件安全模块”)类型。

[0097] 在图3和图4的情况下,安全模块25存储与安全元件2相关联的一组静态钥匙K(并且如已经指出的,还存储在安全元件2的非易失性存储器6中)。应注意,安全模块25存储(或例如,通过从安全元件和主要密钥的标识符推导)一组用于由管理服务器20管理的任何安

全元件的指定的静态钥匙K。

[0098] 如图3和图4所示，设计计算机系统30和安全元件2存储对称密钥K_{0S}，在这种情况下，对称密钥K_{0S}对于大量的安全元件是共用的并且用于加密被安装在这些安全元件上的应用程序部分DATASEND。该共享密钥K_{0S}由安全元件2的制造商管理，并且仍然限制在这些安全元件2和设计计算机系统30内。

[0099] 现给出图3中的解决方案的具体特征的描述。

[0100] 在图3的实施例中，设计计算机系统30还存储一组广播钥匙(或口令密钥)BK，在这种情况下，其包括已经提及的被设计成生成完整性验证码的广播加密或解密钥匙BK-ENC和广播钥匙BK-MAC。这些广播(或口令)密钥BK用于必须接收应用程序部分DATASEND的全部安全元件(也就是说实际上是对其操作系统的更新或对应用程序的其他更新)。

[0101] 因此，设计计算机系统30可以将下列项发送至管理服务器20：

[0102] 通过应用使用广播加密或解密钥匙BK-ENC的(在这种情况下，为对称的)密码加密算法加密的应用程序部分DATASEND；

[0103] 基于广播钥匙BK-MAC和应用程序部分DATASEND确定的完整性验证码MAC；

[0104] 通过应用使用共享密钥K_{0S}的(在这种情况下为对称的)密码加密算法加密的广播钥匙BK-ENC、BK-MAC。

[0105] 应注意，这些元件对于必须接收应用程序部分DATASEND(例如，在这些安全元件的操作系统的更新过程中)的全部安全元件是共用的，并且因此，设计计算机系统30不需要针对被更新的每个安全元件生成应用程序部分DATASEND的加密版本。

[0106] 管理服务器20将加密的广播钥匙BK-ENC、BK-MAC发送至安全模块25，以使得通过应用程序使用会话加密或解密钥匙SK-ENC(在这种情况下为对称的)密码加密算法来加密这些数据。具体地，基于一组静态钥匙K中的静态钥匙K-ENC(存储在安全模块25中并且存储在安全元件2的非易失性存储器6中的静态钥匙)，在安全模块25内与安全元件2内(如上面已经描述的)并行获得该会话加密或解密钥匙SK-ENC。

[0107] 仅以多样化方式加密广播钥匙BK-ENC、BK-MAC、以及完整性验证码MAC(即，通过生成被更新的每个安全元件的加密版本)，并且因此，安全模块25中的处理操作被限制(具体地，是与必须为每个要更新的安全元件生成整个应用程序部分DATASEND的加密版本的情况相比较)。

[0108] 应注意，在该实施例中，通过双层加密形式(通过共享密钥K_{0S}加密并且通过会话钥匙SK-ENC加密)发送广播钥匙BK-ENC、BK-MAC。

[0109] 然后，在根据图2中的步骤E2至E10建立安全链接之后，根据图2中的步骤E14将广播钥匙BK-ENC、BK-MAC从管理服务器20发送至安全元件2。

[0110] 首先，使用会话加密或解密钥匙SK-ENC(如图2的步骤E16中指出的)，并且其次，在这种情况下，使用共享密钥K_{0S}(如已经提及的，存储在非易失性存储器6内)，在安全元件2内解密广播钥匙BK-ENC、BK-MAC。

[0111] 然后，将应用程序部分DATASEND从管理服务器20发送至安全元件2(如上面指出的，通过广播加密或解密钥匙BK-ENC加密的该应用程序部分DATASEND)。

[0112] 安全元件2根据图2中的步骤E22至E26接收、解密、并且存储应用程序部分DATASEND(非易失性存储器6中)(可能被分布至若干块的数据Di的应用程序部分DATASEND，

其中,i＝1,...,N)。

[0113] 然后,安全元件2可以通过会话加密或解密钥匙SK-ENC经由安全信道从管理服务器20接收完整性验证码MAC(在这种情况下,通过对称密钥K_{OS}加密),然后,根据图2中的步骤E32至E36,通过使用完整性验证码MAC和广播钥匙BK-MAC验证应用程序部分DATASEND的完整性。

[0114] 现给出图4中的解决方案的具体特征的描述。

[0115] 在图4的实施例中,设计计算机系统30存储共享的完整性密钥K_{MAC},完整性密钥K_{MAC}存储在大量的安全元件中并且用于验证安装在这些安全元件上的应用程序部分DATASEND的完整性。该共享完整性密钥K_{MAC}由安全元件2的制造商管理并且保持被限制在这些安全元件2与设计计算机系统30内。

[0116] 因此,设计计算机系统30可以将下列项发送至管理服务器20:

[0117] 通过应用使用共享密钥K_{OS}的(在这种情况下,为对称的)密码加密算法加密的应用程序部分DATASEND;

[0118] 基于共享完整性密钥K_{MAC}和应用程序部分DATASEND确定完整性验证码MAC。

[0119] 与管理服务器20相关联的安全模块25其自身存储(一组静态钥匙K除外)广播(或口令)加密或解密钥匙BK-ENC。

[0120] 因此,安全模块25可以根据图2中的步骤E2至E10(通过基于静态钥匙K-ENC生成的会话加密或解密钥匙SK-ENC加密的)与安全元件2建立安全信道,然后,根据图2中的步骤E14经由通过安全元件2接收的该安全信道发送广播加密或解密钥匙BK-ENC。

[0121] 然后,管理服务器20经由根据图2中的步骤E22至E26的多用户安全信道(使用通过广播加密或解密钥匙BK-ENC的加密术)来发送加密的应用程序部分DATASEND(该应用程序部分DATASEND可能被分布至数据Di的多个区块,其中,i＝1,...,N)。

[0122] 应注意,在这种情况下,在通过使用广播加密或解密钥匙BK-ENC的解密算法解密之后获得的数据Di表示(至少部分)通过共享密钥K_{OS}加密的应用程序部分DATASEND。因此,在这种情况下,处理器2还通过应用使用共享密钥K_{OS}的解密算法解密应用程序部分DATASEND。

[0123] 然后,将应用程序部分DATASEND存储在给易失性存储器6中(这与图2中的步骤E26对应)。

[0124] 最后,安全元件2通过会话加密或解密钥匙SK-ENC经由安全信道从管理服务器20接收完整性验证码MAC,并且然后,根据图2中的步骤E23至E36,通过使用完整性验证码MAC和共享的完整性密钥K_{MAC}来验证应用程序部分DATASEND的完整性。

[0125] 应注意,在图3的实施例与图4的实施例中,通过处理器2将所使用的图2中的步骤实现为主要操作系统LOADER的指令的执行结果。

[0126] 而且,在上述的实施例中,会话加密或解密钥匙SK-ENC是通过从存储在安全元件2和期望与安全元件2建立安全信道的电子设备(在这种情况下,为安全模块25)两者中的静态钥匙K-ENC的来源而获得的对称密钥。

[0127] 然而,作为变型,可以规定,在安全元件2中,会话加密或解密钥匙SK-ENC具体是通过是从存储在安全元件2中的私有钥匙k_{SE}的推导而获得的对称密钥,并且在电子设备中,会话加密或解密钥匙SK-ENC具体是根据基于共用钥匙的钥匙协商技术从存储在该电子设备

中的另一私有钥匙K_{EXT}推导而获得的对称密钥，例如文献“Card Secure Channel Protocol'11'Card Specification v2.2-Amendment F(v1.0)”中的规定。

[0128] 图5是示出用于更新安全元件2的操作系统的示例性方法的流程图。

[0129] 该方法从步骤E100开始：在设计计算机系统30内准备要加载到安全元件2的非易失性存储器6中的数据集P_{SE}。

[0130] 在这种情况下，该数据集P_{SE}包含要更新的操作系统的应用程序部分DATASEND。为此，例如，数据集P_{SE}由N个写命令CMDi构成，每个写命令CMDi包含通过广播(或口令)密钥BK-ENC加密的形式的应用程序部分DATASEND的一部分。如图2的步骤E28中提及的，命令CHM(无附加的密钥)还可以放置在N个写命令CMDi的序列的末尾处。

[0131] 广播钥匙BK-ENC用于大量的安全元件，并且因此，准备号的数据将能够以相同的形式被发送到所有这些安全元件(如下文说明的)，以更新其操作系统。

[0132] 在步骤E102中，设计计算机系统30将数据集P_{SE}发送到管理服务器20。

[0133] 管理服务器20在步骤E104中接收数据集P_{SE}，并且在这种情况下在步骤E106中，将该数据集P_{SE}与另一数据集P_{MOB}组合，该另一数据集要被加载在承载安全元件2的用户终端15上(例如，移动电话或蜂窝电话)。

[0134] 在步骤E108中，管理服务器20将数据集P_{SE}、P_{MOB}发送至用户终端15(例如，具体是使用与管理服务器20和安全元件2相关联的移动电话网络)。

[0135] 在步骤E110中，用户终端15接收数据集P_{SE}、P_{MOB}。为此，可以存在例如使得用户终端15的操作从丰富执行环境或REE改变成可信执行环境或TEE(例如，创建为可信操作系统的执行的结果)、并且使得数据集P_{SE}、P_{MOB}被接收在该可信执行环境内的应用(例如，“移动信息装置小程序(midlet)”类型)的执行的上下文中的规定。

[0136] 例如，通过将这些数据存储在用户终端15的存储器中，在步骤E112中，用户终端15从所接收的数据P_{SE}、P_{MOB}提取数据集P_{SE}并且在步骤E114中处理所述其他的数据集P_{MOB}。

[0137] 然后，在步骤E116中，用户终端15将更新的授权请求REQ发送(例如，在操作的随后时刻)至管理服务器20。在步骤E118中，通过管理服务器20接收该请求REQ。

[0138] 然后，在步骤E124中，管理服务器20准备授权数据集P_{AUT}。

[0139] 例如，该授权数据集P_{AUT}包括通过与安全元件2以特定方式相关联的密钥加密的广播钥匙BK-ENC，例如，仅管理服务器20和安全元件2能够生成的会话钥匙SK-ENC。

[0140] 在这种情况下，通过上面参考图2呈现的命令IU、EA、CHM、ATHZ的序列的形式实现授权数据集P_{AUT}。

[0141] 在步骤E128中，管理服务器20将授权数据集P_{AUT}发送至用户终端15。

[0142] 在步骤E130中，用户终端15接收授权数据集P_{AUT}。

[0143] 然后，在步骤E132中，在这种情况下，通过将数据集P_{SE}的命令即时插入在授权数据集P_{AUT}的模式改变命令CHM之后，用户终端15可以组合数据集P_{SE}(在步骤E110中接收并且在步骤E112中提取)与授权数据集P_{AUT}。

[0144] 具体地，如上所述，通过多个安全元件(实际上，大量的安全元件)共享的广播钥匙BK-ENC加密数据集P_{SE}的命令中包含的数据，并且因此，在将安全元件2切换至多用户模式之后，不得不接收这些命令。

[0145] 在步骤E134中，用户终端15将在步骤E132中准备(通过组合)的命令发送至安全元

件2。为了简单起见，仅在图5的一个步骤中示出了这些命令的连续发送。实际上，每个步骤从用户终端15被单独发送至安全元件2。

[0146] 如上面参考图2描述的(通过步骤E136示意性示出的)，安全元件2连续接收并且执行各个命令。

[0147] 如上面关于图2中的步骤E40说明的，在执行全部命令时，安全元件2发送一条静态信息ST(步骤E138)。

[0148] 在步骤E140中，通过用户终端15接收该条静态信息ST，并且在步骤E142中将该条静态信息ST发送至管理服务器20。

[0149] 在步骤E144中，管理服务器20接收该条静态信息ST，并且如果该条静态信息ST确认正确更新安全元件ST的操作系统，管理服务器20则通过例如授权配备有安全元件2的用户终端访问移动电话网络而基于该条静态信息ST执行处理操作，并且如果该条静态信息ST不确认正确更新，管理服务器20则通过执行其他动作(例如，新尝试加载，阻碍当前讨论的用户终端15访问网络)而执行处理操作。

[0150] 例如，授权数据P_{AUT}使得可以激活由数据集P_{SE}、P_{MOB}定义的功能。

[0151] 由此，刚刚描述的方法使得可以在激活这些功能之时的时刻最小化交换。具体地，通过在步骤E100至E114中预先加载数据集P_{SE}、P_{MOB}，仅在激活时刻发送的数据成为授权数据P_{AUT}。

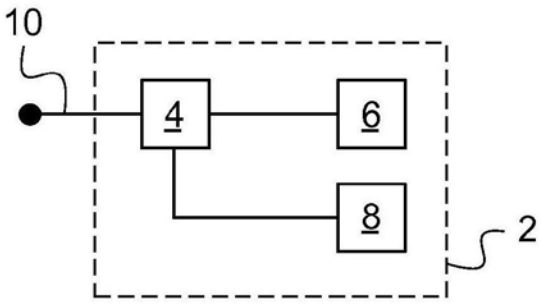


图1

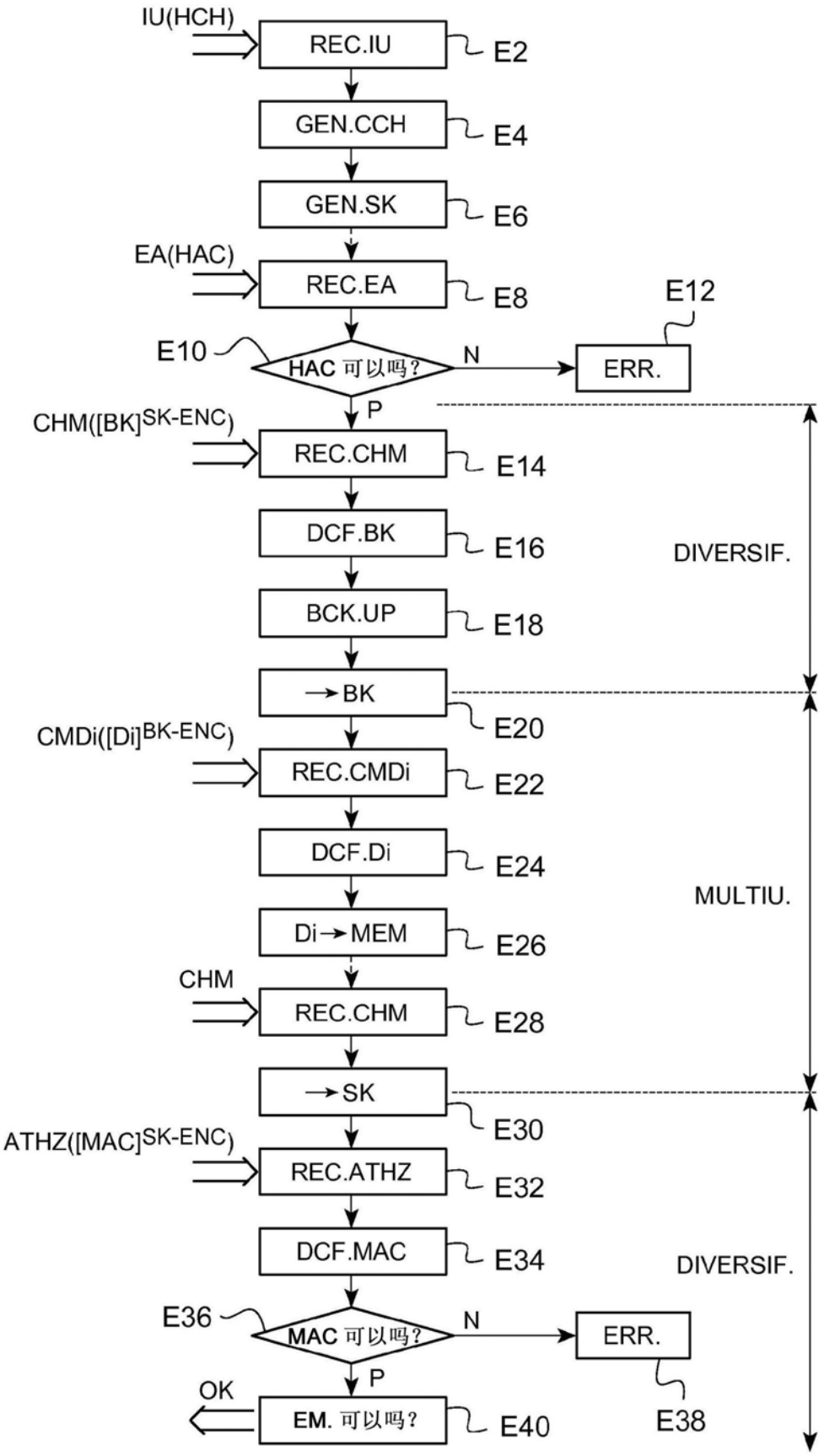

IU(HCH)
REC.IU
E2
GEN.CCH
E4
GEN.SK
E6
EA(HAC)
REC.EA
E8
E12
E10
HAC 可以吗?
N
ERR.
P
CHM([BK]SK-ENC)
REC.CHM
E14
DCF.BK
E16
DIVERSIF.
BCK.UP
E18
→BK
E20
CMDi([Di]BK-ENC)
REC.CMDi
E22
DCF.Di
E24
MULTIU.
Di→MEM
E26
CHM
REC.CHM
E28
→SK
E30
ATHZ([MAC]SK-ENC)
REC.ATHZ
E32
DCF.MAC
E34
DIVERSIF.
E36
MAC 可以吗?
N
ERR.
E38
P
OK
EM. 可以吗?
E40

图2

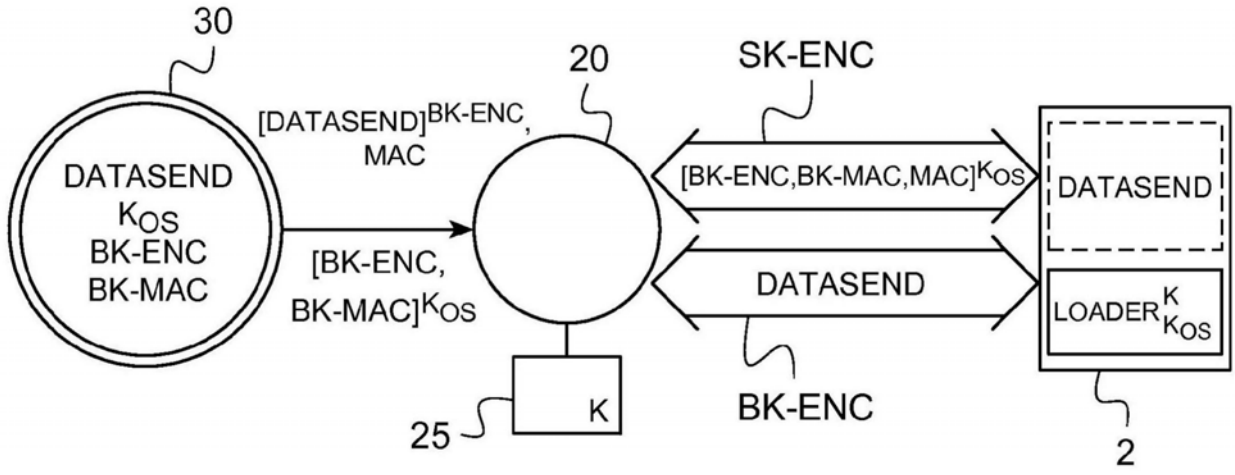

30
DATASEND
K_{OS}
BK-ENC
BK-MAC
[DATASEND]BK-ENC, MAC
[BK-ENC, BK-MAC]K_{OS}
20
SK-ENC
[BK-ENC,BK-MAC,MAC]K_{OS}
DATASEND
BK-ENC
DATASEND
LOADER K_{OS}
K
25
2

图3

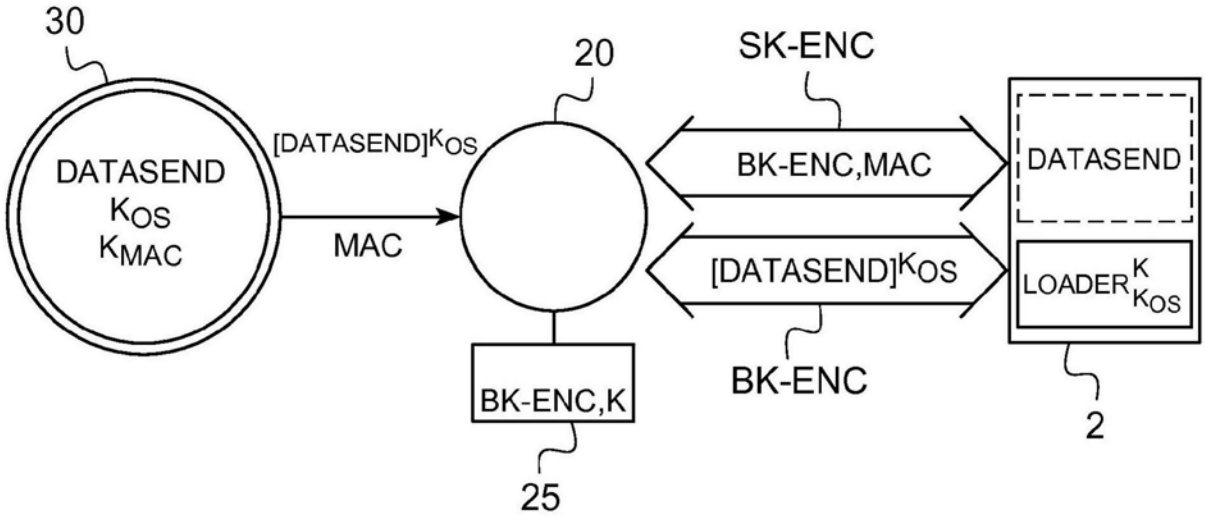

30
DATASEND
K_{OS}
K_{MAC}
[DATASEND]K_{OS}
MAC
20
SK-ENC
BK-ENC,MAC
[DATASEND]K_{OS}
BK-ENC
DATASEND
LOADER K_{OS}
BK-ENC,K
25
2

图4

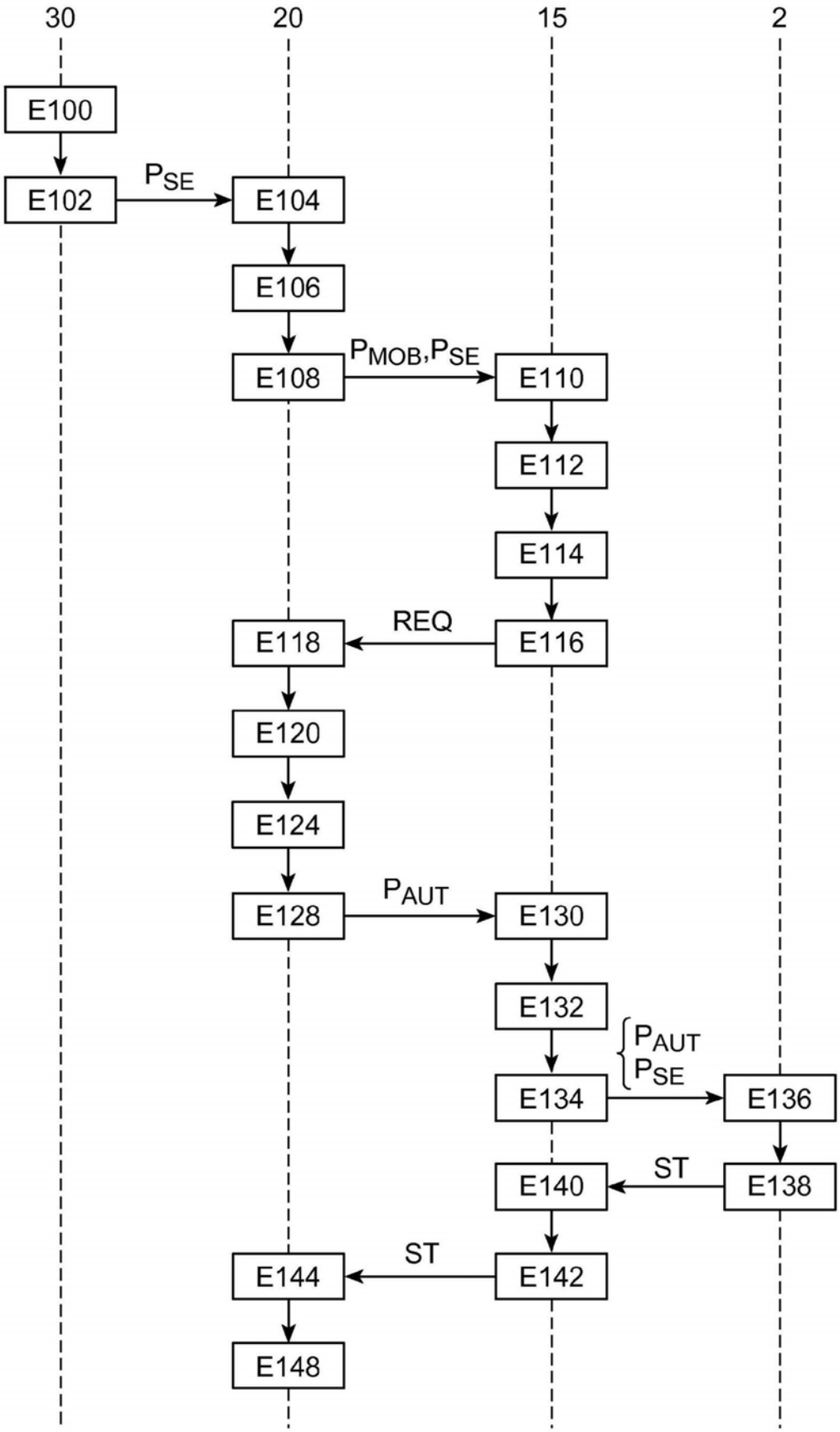

30
20
15
2
E100
E102
PSE
E104
E106
E108
PMOB,PSE
E110
E112
E114
E116
REQ
E118
E120
E124
E128
PAUT
E130
E132
PAUT
PSE
E134
E136
E138
ST
E140
E142
ST
E144
E148

图5