(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 108432207 B
(45)授权公告日 2021.02.09

(21)申请号 201680076955.2
(22)申请日 2016.12.22
(65)同一申请的已公布的文献号
申请公布号 CN 108432207 A
(43)申请公布日 2018.08.21
(30)优先权数据
15382665.6 2015.12.28 EP
(85)PCT国际申请进入国家阶段日
2018.06.28
(86)PCT国际申请的申请数据
PCT/EP2016/082298 2016.12.22
(87)PCT国际申请的公布数据
WO2017/114731 EN 2017.07.06
(73)专利权人 莱里达网络远程信息技术服务有限公司
地址 西班牙莱里达
(72)发明人 F·萨佩纳索勒尔
(74)专利代理机构 余姚德盛专利代理事务所(普通合伙) 33239
代理人 郑洪成
(51)Int.Cl.
*H04L 29/06*(2006.01)
*H04L 12/58*(2006.01)
(56)对比文件
US 2012272063 A1,2012.10.25
EP 2632096 A1,2013.08.28
CN 104145454 A,2014.11.12
US 2015312233 A1,2015.10.29
CN 103716228 A,2014.04.09
US 2010100465 A1,2010.04.22
审查员 刘金鑫

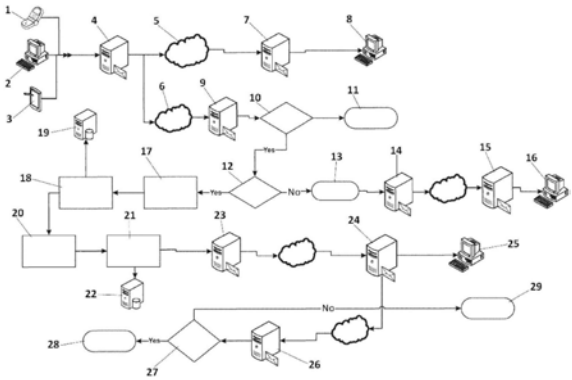
权利要求书2页 说明书5页 附图2页

(54)发明名称

通过电信运营商进行的数字签名的电子邮件的认证方法

(57)摘要

本发明的目的是用于认证具有经认可电子签名的电子邮件的方法,其中电信运营商认证将所述运营商的用户客户端部分上的经认证电子邮件发送给该电信运营商的另一个用户非客户端,在重新发送和认证中始终尊重监管链和原始的经认可电子签名,在交易的任何时候都可以产生证据,以便可以在任何法庭中用作强化证据或作为给定交易的可靠的证明。




CN 108432207 B

1.通过电信运营商进行的数字签名的电子邮件的认证方法，该方法包括：

i.由作为所述电信运营商的用户的发送方(1,2,3)生成至少一个电子邮件，

ii.使所述电子邮件到达所述电信运营商的客户端邮件服务器(4,15)，

iii.发送所述电子邮件至：

- 通过互联网(5)到邮件目的地服务器(7,24)，使其到达经认证的邮件目的地(8,25)，以及

- 所述运营商的接收邮件服务器(9)，

iv.证明(17)所述电子邮件，其中所述证明又包括生成所述电子邮件的副本(18)并将所述电子邮件分解成其部分，其中所述部分包括：传输细节、邮件的接收细节和内容，

数字签名电子邮件的认证方法的特征在于它包括：

i.一旦所述副本(18)已被分解，则执行将所述电子邮件及其部分的副本(18)转储到第一数据库(19,32,43)，

ii. 还包括在第二数据库(22,33,46)中执行经认证邮件(21)的转储，所述第二数据库包括已经被做成到达所述运营商的外发邮件服务器(23,26,38,50)的元素，

iii.将所述电子邮件的副本(18)封装(20)在容器中，

iv.生成包括电子邮件的封装副本(18)的经认证邮件(21)并使所述经认证邮件(21)到达运营商的外发邮件服务器(23,26)，

v.使得所述经认证邮件(21)从运营商的外发邮件服务器(23,26,38,50)到达所述邮件目的地服务器(7,24)，

vi.使得所述经认证邮件(21)从所述邮件目的地服务器(7,24)到达：

a. 经认证邮件目的地(8,25)，以及

b. 所述运营商的外发邮件服务器(23,26,38,50)，

vii.在所述经认证邮件目的地(8,25)进行所述经认证邮件(21)的送达检查(27)，

viii.借助于所述电信运营商的认证服务器(30,41)生成证书(37,49)，其中所述证书包括：

a.第一部分(31,42)，其又包括：发送细节、邮件的接收细节和内容，以及

b.第二部分(34,45)其又包括所述证书(21)到达运营商的外发邮件服务器(23,26)的细节，以及

c.所述电信运营商的数字签名和时间戳(35,48)，以及

ix.使所述证书(37,49)到达所述发送方(1,2,3)。

2.根据权利要求1所述的方法，其特征在于，还包括通过与用户/特权列表的比较检查(10)发送方(1,2,3)具有认证特权，通过将电子邮件发送到认证数据处理服务器来进行检查。

3.根据前述权利要求中任一项所述的方法，其中，步骤vii的所述送达检查(27)作为结果在所述经认证邮件目的地(8,25)处未送达所述经认证邮件(21)，所述方法被表征此外它还包括向证书(37,49)添加涉及未送达的细节，其中所述细节包括：尝试送达的时间和送达地址。

4.根据权利要求1所述的方法，其中，步骤xi的所述送达检查(27)作为结果在所述经认证邮件目的地(8,25)处递送所述经认证邮件(21)，所述方法的特征在于：另外它包括在步

骤viii.a中生成第一部分(31,42)之后的验证(44),其中所述验证(44)包括检查经认证邮件目的地服务器(8,25)是否在弹跳/列入黑名单服务器的列表上,所述弹跳/列入黑名单服务器在默认情况下接受所有消息,并在相应的经认证邮件收件人(8,25)不存在时稍后拒绝。

5.根据权利要求4所述的方法,其中所述验证(44)作为结果给出所述经认证邮件目的地服务器(8,25)位于弹跳/列入黑名单服务器的列表上,所述方法的特征在于,另外它包括向所述证书(37,49)添加涉及在经认证邮件目的地服务器(8,25)上不存在收件人的详情。

# 通过电信运营商进行的数字签名的电子邮件的认证方法

## 技术领域

[0001] 本发明的目的是一种用于电信运营商能够非侵入性地接收，重定向，递送和认证使用该运营商的任何发送用户客户端的经认可电子签名签署的电子邮件给运营商的一个或多个接收方非客户端的方法，尊重原始邮件的电子签名以避免打破监管链，将其与原始签名一起完整地重新发送并适应DMARC标准，从而生成所有操作事务的证明，以便最终作为电信运营商以数字方式对其签名并作为可信的第三方向发送用户客户端递送证书，其中包括发送方的详细信息、传输日期、发送的全文、用户以电子方式尊重原始签名所签署的原始邮件、递送日期和时间以及在未递送或延迟递送给非客户端接收方的情况下的最终情形。

## 背景技术

[0002] 众所周知，目前电子通讯已成为任何合法和非法操作的基本和不可或缺的工具。通信用于从起点到目的地的所有类型的移动、呼叫的生成、消息等等。

[0003] 电信运营商是提供管理，指导和存储很大一部分此类流量的基础设施的各方。除其他外，这些电信运营商受限于使用有限的无线电频谱或使用也是有限的电话号码资源的规定等等。

[0004] 电信运营商还登记由用户进行的操作，其中目标包括收费，注册与其相关的号码等作为账单参考，并记录任何其他用于对用户收费的交易细节。这些登记被保存以用于后续验证费用和/或监控用户部分的流量。

[0005] 有时，司法当局要求电信运营商提供电子交易的登记细节，因为他们认为这些电子交易是可信的第三方以提供这些细节，以及任何其他可能有助于确定已经执行了感兴趣的动作的私人个体或法人实体的细节。

[0006] 一旦司法当局要求的详细信息被查找到，运营商就会发布证书，明确声明所请求的交易细节、频率、目的地以及相关司法当局所要求的任何其他信息。

[0007] 这种方法在电信运营商的任何一方提出要求并作为证据提出时，甚至最近都被我们的最高法院接受为证据(ATS 2501/2013，西班牙最高法院民事法庭)。

[0008] 现有技术熟悉用于发送经认证的电子邮件的各种方法和系统，一些方法和系统基于客户端的部分发送链接到受信任的第三方控制的网络环境，在该网络环境中认证的内容被下载，具有要求被通知方的意愿下载所述内容以便生成证书的基本缺点，以及其它方法和系统是数字验证被添加到内容并且被模拟为发送方将其重新发送到目的地。最后一个有三个严重的缺点：

[0009] a)在代表用户重新发送时，经认可的电子签名被破坏，原因是条件完全改变，打破了监管链并产生了不信任。

[0010] b)在内部添加验证以便随后再次检查电子邮件的认证时，再次打破原来经认可的电子签名和监管链。

[0011] c)在好像用户一样代表用户重新发送时，经认证电子邮件与全球范围内作为标准强加的DMARC标准发生冲突，从而阻止了经认证的电子邮件的有效递送。

[0012] 作为本申请的目的的发明提供了对上述缺点的解决方案,不需要随后下载待认证的内容,尊重用户的原始经认可的电子签名以维持监管链,以及在DMARC标准下的服务的完整的功能;通过该过程产生由电信运营商发布的包含原始消息的证书,而不会破坏原始经认可的签名,该原始经认可的签名确认运营商在确定的日期和时间将该电子邮件内容发送到目的地,并且该签名最终被递送或不递送给其官方电子代表,包括传输详情、传输的详细信息、附件、单一注册号以及所使用的任何交易细节。

[0013] 发明概述

[0014] 根据上述内容,本发明的目的是一种发送电子邮件的方法,电子邮件具有经认可电子签名以便由通信运营商以这样的方式进行认证,即目的地接收两个副本,来自客户端的原件以及来自电信运营商的未经模拟成为原始客户端的副本,尊重经认可电子签名和监管链。运营商或发送方的客户端根据发送原始电子邮件的人员接收证书,包括原始邮件,可查看内容,日期,时间及其可追溯性,单个交易号码;最后是送达的日期、时间和情况(如果可能的话)。

[0015] 用于创建作为本发明的目的的电信运营商认证的电子邮件的方法的特征在于,其包括以下步骤,并且其包括运营商的客户端的至少一个外部邮件服务器,经认证邮件的目的地服务器,运营商的传入邮件服务器,副本和分段元素的数据库服务器,运营商的外发邮件服务器,TSA时间戳服务器,发送的元素的数据库服务器以及作为认证服务器的数据处理单元,所有这些彼此互连。

[0016] -电信运营商的客户端通过他们的互联网提供商将电子邮件发送到使用任何平台的确定目的地,复制电信运营商服务器的邮件地址,例如 correo@certificado.lleida.net

[0017] -通过其授权的数字代表在目的地收到传统电子邮件。

[0018] -接收电信运营商的用户客户端发送的消息在运营商的传入邮件服务器中的副本。

[0019] -检查用户是否被授权,有资格认证邮件并转到在收到的文本和组件的数据库中插入和注册。

[0020] -在电信运营商的数据处理单元中创建电子邮件的数据处理单元,该电子邮件将从电信运营商的服务器的地址noreply@mailcert.lleida.net发送,封装运营商客户端发送的内容以尊重经认可的原始数字签名,专门插入电子邮件的主题经认证电子邮件(CERTIFIED ELECTRONIC MAIL)中。

[0021] -外发电子邮件服务器部分上的封装的邮件的发送。

[0022] -接受或不接受封装电子邮件的非客户端目的地的授权数字代表,

[0023] -最终生成电信运营商的证书,包括尊重经认可数字签名的原始邮件,发送、收到的细节,发送和接收的日期和时间以及电信运营商部分的经认可数字签名以及时间戳的应用。

[0024] -通过邮件服务器向发送用户发送证书。

[0025] 根据以上所述,作为本发明目的的方法同样提供了不操纵原始邮件,保持监管链并允许使用用户认可的数字形式,同样与DMARC标准兼容的优点,因为邮件的封装副本不是以用户的名义重新发送,而是以电信运营商的名义重新发送。最后,证据是由电信运营商部

分的内容发送、接收和接受而产生的。

## 附图说明

[0026] 为了补充正在进行的描述并为了有助于更好地理解本发明，根据其实际实施方案的优选实施例，附有一组附图作为所述描述的组成部分，其中作为说明而不是限制，已经表示如下：

[0027] 图1示出了作为开始创建经认证的电子邮件和封装副本的送达或未送达的发明的目的的方法的实施方案的实施例的流程图。

[0028] 图2示出了作为本发明的目的的、封装电子邮件的送达或未送达情况下的最终证书的撰写和发送的方法的实施方案的实施例的流程图。

[0029] 发明详述

[0030] 根据图1和图2，其中一系列图表是参照作为本发明的目的的方法来表示的，方法旨在认证包含电信运营商方面的经认可电子签名的电子邮件的方法，包括从从发送方(1,2,3)即电信运营商的用户发送电子邮件到接收确认发送已完成的证书，它已被送达以及所使用的内容和传输细节的证书，所有上述信息都被运营商的经认可电子签名和第三方的时间戳进行签署。

[0031] 当希望发送经认证电子邮件时，电信运营商的发送用户客户端通过任何平台、PC、平板电脑或移动电话发送邮件，复制电信运营商的传入邮件服务器的邮件地址，例如correo@certificado.lleida.net。为此，在作为电信运营商的用户的发送方(1,2,3)的部分上，生成至少一个电子邮件，以使电子邮件到达电信运营商(4,15)的客户邮件服务器，例如电子邮件被发送到Lleida.net的客户端邮件服务器，Lleida.net的客户端邮件服务器属于任何互联网提供商，并且为了合法目的而将其送达目的地服务器是授权的电子代表，换言之，通过互联网(5)使其到达邮件目的地服务器(7,24)，以使其到达经认证的邮件目的地(8,25)，因为它处于互联网级别，在该级别处可将消息递送到一个确定的目的地，同样这个消息的副本被递送到运营商(9)的传入邮件服务器，在这个实施例中是Lleida.net的传入邮件服务器。

[0032] 运营商的传入邮件服务器(9)将电子邮件发送到构成电信运营商的一部分的认证数据处理服务器(Mailcert)，并且将检查用户是否在白名单上，换句话说，向系统注册以便能够发送经过认证的电子邮件。如果未注册，则邮件将被忽略，如果注册它将继续验证用户是否具有信用，这意味着通过与用户/特权列表比较来检查(10)用户(1,2,3)具有认证权限，检查通过将电子邮件发送到认证数据处理服务器来执行哪一个。

[0033] 如果所讨论的用户没有任何信用，就会生成一个电子邮件，说明缺少信用，将其发送给运营商的外发邮件服务器(23,26,38,50)，外发邮件服务器最终将其送达用户(1,2,3)，该用户是通信运营商的用户客户端。

[0034] 如果用户确实有信用，那么它继续认证(17)电子邮件，其中所述认证又包括生成电子邮件的副本(18)并将电子邮件分解成其部分，其中所述部分包括：发送细节，用于其处理的邮件的接收细节和内容，所述细节优选与副本(18)一起保存在第一数据库(19,32,43)中。

[0035] 随后，将电子邮件的副本(18)封装(20)在容器中，并且生成经认证的邮件(21)，该

邮件包括电子邮件的封装后的副本(18)，然后使其到达运营商(23,26)的外发邮件服务器，从运营商的外发邮件服务器 (23,26,38,50)到达邮件目的地服务器(7,24)，并使得经认证的邮件(21) 从邮件目的地服务器(7,24)到达:经认证的邮件目的地(8,25)，以及运营商的外发邮件服务器(23,26,38,50)。

[0036] 经认证邮件(21)由电子邮件地址生成，源自认证数据处理服务器，该服务器构成电信运营商的一部分，可能是:service@correoelectrónicocert.lleida.net，消息主题为CERTIFIED ELECTRONIC MAIL，添加原始主题的文本，以及可能认为必要的尽可能多的控制文本。从电信运营商作为认证服务器服务@correoelectrónicocert.lleida.net发送的事实，以及未将客户端的原始电子邮件地址作为原电子邮件地址发送的事实允许该服务符合DMARC标准，因为它不代替客户端，尽管授权我们代表客户端递送电子邮件。

[0037] 在通过认证的邮件(21)的文本中包含一个标语，并指示确认它是一个经认证的消息，最后将其封装(20)，换句话说，为了尊重原始经认可电子签名目的以避免任何内部操纵破坏经认可签名并且产生对消息真实性的不信任而包含了整个原始消息。电子邮件的封装后副本(18)被保存在第二数据库(22,33,46)中并且被送到运营商的外发邮件服务器 (23,26,38,50)以发送它。

[0038] 运营商的外发邮件服务器(23,26,38,50)将递送电子邮件的封装后副本(18)以供其递送，但即使如此也将等待随后的10分钟至1小时之间的时间以供后续拒绝响应，换句话说，最初在目的地的电子邮件服务器将首先接受所有内容，随后它将拒绝它，这是系统自动地自调整的行为。

[0039] 如果认证的电子邮件最终能够送达，则该方法转到图2的确认(OK) 过程，并且如果经认证的电子邮件不能被送达，则它继续进行也在图2中呈现的未确认(NOOK)过程。

[0040] 运营商的外发邮件服务器(23,26,38,50)将封装的电子邮件递送给其授权的数字代表以供其递送，但即使如此，也将等待随后的10分钟至1 小时之间的时间以供后续拒绝响应，换句话说，最初邮件目的地服务器 (7,24)首先接受所有内容并且随后拒绝它，这是这里描述的方法自动地自调整的行为。

[0041] 在经过认证的邮件目的地(8,25)，检查经认证邮件(21)的送达(27)。如果最终能够送达经认证的邮件(21)，则该方法转到图2的OK过程，并且如果经认证的电子邮件不能被送达，则该方法继续进行也在图2中呈现的NOOK过程。

[0042] 通过送达经认证邮件(21)，该方法进入到生成运营商本身的证书 (37,49)的过程中，换句话说，使得经认证邮件(21)从邮件目的地服务器(7,24)到达经认证邮件目的地(8,25)并且到达运营商外发邮件服务器(23,26,38,50)，因为在经认证邮件目的地(8,25)处执行经认证邮件(21) 的送达检查(27)时，获得了OK。接下来，通过电信运营商的认证服务器(30,41)生成证书(37,49)，其中所述证书(37,49)包括第一部分(31,42)，该第一部分又包括发送细节、接收细节和邮件内容，以及第二部分(34,45)，第二部分又包括证书(21)到达运营商的外发邮件服务器(23,26)的详细信息，以及电信运营商的数字签名和时间戳(35,48)。

[0043] 为此，内容和原始电子邮件从构成证书(37,49)第一部分的初始副本的第一数据库(19,32,43)中恢复。一旦完成，通过在生成第一部分(31,42) 之后的验证(44)来验证邮件目的地服务器(7,24)是否在弹跳/列入黑名单列表中，其中所述验证(44)包括检查经认

证的电子邮件(8,25)的目的地服务器是否在弹跳/列入黑名单服务器的列表上,弹跳/列入黑名单服务器默认接受所有消息并且随后在相应的经认证邮件(8,25)的收件人不存在时拒绝它们。换句话说,验证(44)是否在默认接受所有消息并且稍后在用户不存在时拒绝它们的服务器列表上,检查是否有来自邮件目的地服务器(7,24)的后续拒绝消息。如果后来的拒绝信息已经到达,那么该方法进入NOOK过程。

[0044] 如果验证(44)作为结果给出经认证的邮件目的地服务器(8,25)在弹跳/列入黑名单服务器列表上,则继续向证书(37,49)添加涉及认证的邮件目的地服务器(8,25)上不存在收件人的详情。如果验证(44)作为结果给出邮件目的地服务器(7,24)不在黑名单或弹跳清单上,则证书的第二部分由所有交易详情构成,添加第三方的时间戳(35,48)并且如前在描述证书(37,49)的第二部分(34,45)的内容时所述,用电信运营商的经认可电子签名来签署该证书(37,49)。

[0045] 完成证书(37,49)后,生成一个电子邮件,附上这个生成的证书 (37,49),发送给电信运营商的外发邮件服务器(23,26),外发邮件服务器最终将其发送给经授权将其送达客户端的电子代表。

[0046] NOOK过程是在任何情况下都不能将经认证邮件(21)发送到经认证的邮件目的地(8,25)时所使用的过程,强调在发送可靠通知的过程中,送达和未送达也同样重要,因为其目的是为了证实发送内容的公开显式和明确的意愿,即使可能存在阻止该内容的情况,也会将可靠的通知转化为勤勉的通知;换句话说,在技术上可行的一切都已经完成以实现送达。

[0047] 一旦确定经认证邮件(21)进入NOOK过程,证书(37,49)再次重新编写,以识别收件人并在证书(37,49)中包含收件人的详细信息以及防止将消息有效送达其授权的电子代表的所有变化,例如可以在证书(37,49) 中添加涉及未送达的细节,例如尝试送达的时间,送达地址,收件人的身份等。一旦证书(37,49)完成,它将通过电信运营商的经认可数字签名进行电子签名,并向其中添加第三方的时间戳。

[0048] 一旦文件被签署,就会生成一个电子邮件,并附上该pdf文件,并通过电子邮件发送给作为电信运营商的用户的发送方(1,2,3)。

[0049] 利用最终生成的证书(37,49),作为电信运营商的用户的发送方(1,2,3) 能够可靠地证明其发送了经认证邮件(21)到确定的经认证的邮件目的地 (8,25),使用其自己的经认可的电子签名而不修改其任何交易中的电子邮件,或由于在互联网上实施新标准而阻止其送达。

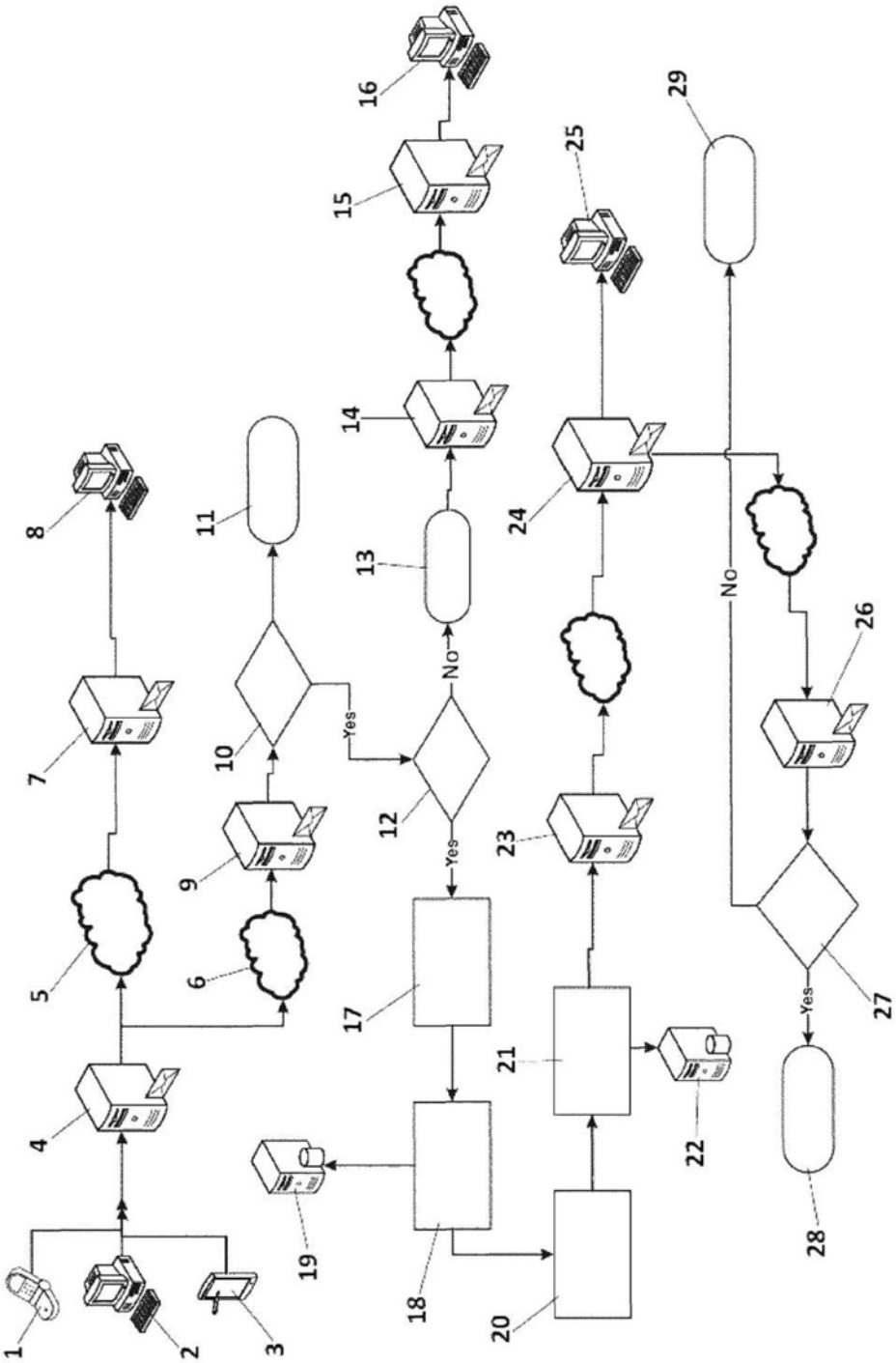

1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28
29
Yes
No
Yes
No
Yes

图1

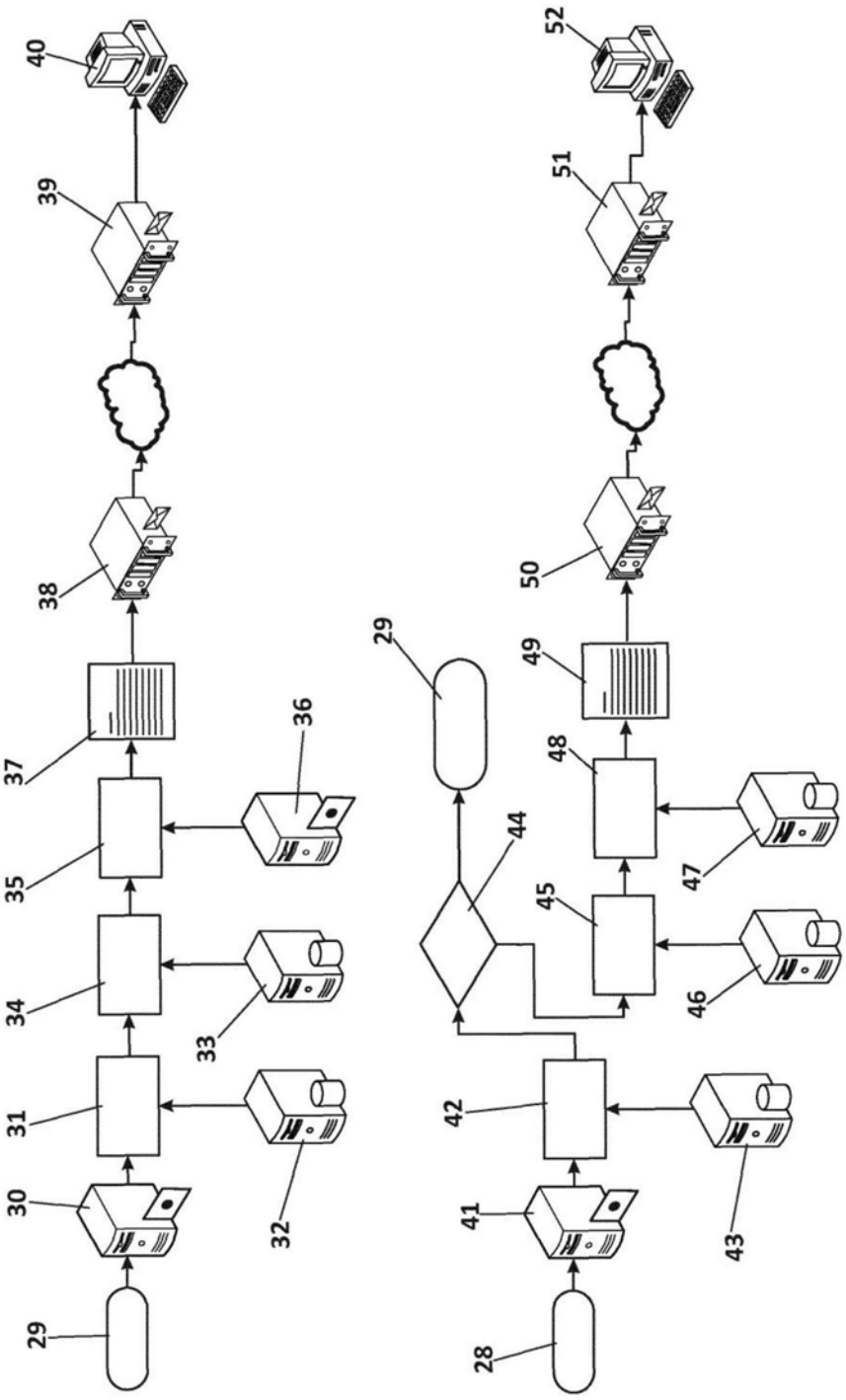

40
39
38
37
36
35
34
33
31
32
30
29
52
51
50
49
48
47
45
46
44
42
43
41
28
29

图2