(19)中华人民共和国国家知识产权局

(12)发明专利申请

(10)申请公布号 CN 111480321 A
(43)申请公布日 2020.07.31

(21)申请号 201880065807.X

(22)申请日 2018.08.20

(30)优先权数据
17382631.4 2017.09.21 EP

(85)PCT国际申请进入国家阶段日
2020.04.09

(86)PCT国际申请的申请数据
PCT/ES2018/070562 2018.08.20

(87)PCT国际申请的公布数据
WO2019/058006 ES 2019.03.28

(71)申请人 莱里达网络远程信息技术服务股份有限公司
地址 西班牙莱里达

(72)发明人 F·萨皮纳索勒

(74)专利代理机构 上海专利商标事务所有限公司 31100
代理人 蔡悦 陈斌

(51)Int.Cl.
H04L 12/58(2006.01)
H04L 29/06(2006.01)
H04W 4/14(2006.01)
H04W 12/06(2006.01)
G06Q 10/10(2006.01)
G06F 21/33(2006.01)

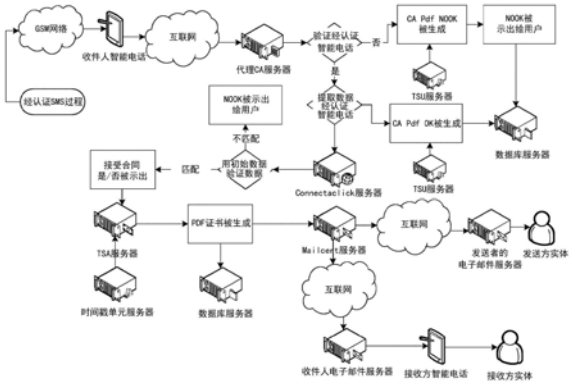
权利要求书2页 说明书5页 附图3页

(54)发明名称

用于电子标识和信任服务(EIDAS)的电子合同的认证的平台和方法

(57)摘要

本发明的目的涉及一种方法,该方法允许电信运营商或电子通信提供商(诸如提供电子交付的电信运营商)通过电子邮件向一个或数个收件人发送合同,认证合同内容且具有到将验证收件人的数字证书及其身份的认证机构(CA)的代理服务器的链接,将通信重新发送到其中合同可以被验证、接受或拒绝的合同服务器,并作为通信运营商生成交易的证明,其中合同、签订合同实体、CA签发的与签订合同实体相关的证书以及展示该交易所需的所有交易数据被找到。



CN 111480321 A

1.一种认证电子合同的平台,其特征在于,包括与通信提供商相关联且彼此连接的下列各项:

• 实现电子合同电子邮件系统的合同服务器,

• 具有收集证据的能力的电子邮件管理服务器,

• 用于存储原始电子邮件的内容的数据库服务器,

• 时间戳服务器,

• 用于生成在合同过程期间收集到的证据的服务器,

• 通过使用被包含在接收者的浏览器中的数字证书来负责确保收件人的身份的确认服务器,

• 负责发送经认证消息的经认证消息服务器,以及

• 用于存储由文档生成服务器生成的电子合同证书的经生成文档服务器。

2.一种认证电子合同的方法,其特征在于,所述方法包括通过通信提供商:

• 由发送方即发送方实体的用户访问合同服务器,

• 引入接收者即接收方实体的用户的数据,其中所述数据包括以下至少一者:收件人电子邮件地址和收件人电话号码,

• 选择收件人电话号码或收件人电子邮件地址,

• 向所述接收者发送:通过经认证SMS服务器的SMS或通过电子邮件管理服务器的经认证电子邮件,其中经认证SMS和经认证电子邮件都包括至少一个URL,所述至少一个URL链接到CA(认证机构)服务器的代理服务器,通过所述代理服务器,所有通信被执行,

• 由所述接收者访问所述URL,并选择要在交易中被使用的优选地被包含在浏览器中的数字证书。

• 由所述收件人通过CA的代理服务器访问所述合同服务器以验证所述数字证书中所包含的数据,

• 由所述接收者签署所述合同,

• 将经签署合同的副本发送给所述接收者,

• 由证据生成服务器生成证据,

• 通过所述证据生成服务器生成具有所有网络数据、所述合同、CA的代理服务器所生成的文档以及所使用的操作的交易数据的交易证书,

• 利用所述通信提供商的数字签名来签署所述交易证书,

• 一旦所述交易证书已被签署,通过时间戳服务器将时间戳应用于所述交易证书,以及

• 发送所述交易的经签署且经加戳的证书的至少两份副本和所有经生成的证据,一份发送给发送方实体,而另一份发送给接收方实体,以便由其各自的用户收集。

3.根据权利要求2所述的方法,其特征在于,在不存在数字证书或对所述数字证书的访问的情况下,所述方法包括:

• CA的代理服务器确定所述过程无法继续,

• 由所述代理服务器生成不合规文件,

• 将所述不合规文件存储在所述经生成文档服务器中,以及

• 对所述经生成文档服务器中的所述不合规文件加盖时间戳。

4.根据权利要求2或3所述的方法，其特征在于，所述方法还包括通过与初始引入的数据进行比较来验证所述浏览器的证书中所包含的数据。

用于电子标识和信任服务(EIDAS)的电子合同的认证的平台和方法

[0001] 发明目的

[0002] 本发明的目的是在信息和通信技术领域的框架内的。

[0003] 更具体而言,此处所描述的方法针对用于认证电子文档的介入方、发送、接收和内容的应用。

[0004] 发明背景

[0005] 数字证书和合同的领域如今已发展了很多年;然而,在数字证书领域的参与者中存在着在证书机构、数字公司、电子交付提供商、认证过程、可认证的过程以及不同方法之间的普遍混淆。另外,经数字签名的文档仅包括有关谁对它们签名并且其内容被保持未经修改的信息,但如果其他数字手段被用来接受和数字地签署合同,则它们不包含有关它们的发送、交付、接受或拒绝的信息。

[0006] 用于合同的最常见方法一直是到场通知并集中所有动作,使用单个CA用于证书、签名,并且这些事情全部在一个地点进行。就其本身而言,这可能是其中先验知识最简单的方法,但问题在于,所需证书、需要签名的地方以及在准备到场通知时为避免丢失通知而需要数字存在或定期访问的位置的数目成倍增加。仅在西班牙,如果希望在全国范围内运营,则存在约80000个数字实体是必须访问的。

[0007] 前面提到的缺点必须被解决,并允许使用在代理CA中被配置的任何数字证书,以使得可以通过电子邮件和SMS随时发起过程;存在对所有已采取的步骤的记录,以使得可以随时展示合同过程的参与者是谁以及合同过程已在什么时候进展以及进展到什么地步。

[0008] 电子信任(trust)服务包括:

[0009] • 电子签名、电子戳或电子时间戳、经认证电子交付服务以及与这些服务相关的证书的创建、验证和确认。

[0010] • 用于对网站进行认证的证书的创建、验证和确认。

[0011] • 与这些服务相关的签名、戳或电子证书的保存。

[0012] 从这个意义上讲,电子标识和信任服务(eIDAS)框架必须被建立,通过实施eIDAS,针对电子交易的电子标识和信任服务被监督。eIDAS规定了电子签名、电子交易、所涉及的主体以及其包括过程,用于为用户提供安全方式来进行在线业务,诸如利用公共服务进行电子转账或交易。签名者和收件人都能够使用更高级别的便利性和安全性。替代依靠于传统方法(诸如电子邮件、传真服务或亲自到场以出示纸质文档),现在可以例如使用“一键式(1click)”技术来执行跨境交易。

[0013] 因此,eIDAS的实施建立了电子签名、合格的数字证书、电子戳、时间标记和其他用于认证机制的测试的标准,这些标准允许与纸面上所执行的交易具有相同合法性的电子交易。

[0014] 发明描述

[0015] 在本发明的第一方面中,提供了一种用于认证电子合同的平台,该平台通过电信运营商利用一系列互连服务来实现。该平台可由此具有使得其实现下列各项的配置:实现

电子合同电子邮件系统的合同服务器、带有证据收集的电子邮件管理服务器、存储原始电子邮件内容的数据库服务器、时间戳服务器、用于生成在合同过程期间收集到的证据的服务器，通过使用被包含在接收者的浏览器中的数字证书来负责确保收件人的身份的确认服务器、负责发送消息的经认证消息服务器、以及用于存储由文档生成服务器生成的电子合同证书的经生成文档的服务器。

[0016] 应该提到的是，由于平台被连接到电信运营商(或本文全文中的通信运营商)，并且优选地被实现在其中，因此这允许认证任务被执行而无需通信运营商外部的网络实体。

[0017] 在本发明的第二方面，本发明的目的涉及一种方法，其中电信运营商或电子通信提供商(电子交付提供商)可以通过电子邮件向一个或数个收件人发送合同，使用到将验证收件人的数字证书及其身份的CA(认证机构)的代理服务器的链接来证明合同内容，将通信重新发送到其中合同可以被验证、接受或拒绝的合同服务器，并作为通信运营商生成交易的证明，其中合同、签署合同实体、CA签发的与签署合同实体相关的证书以及展示该交易所需的所有交易数据被找到。

[0018] 本发明的目的是提供一种用于在两端使用稳健的标识对以电子方式执行的合同进行认证的方法；通过CA将检查的签名的数字证书的对客户端的标识、以及通过将服务签约给电子交付提供商、通信或电信运营商的对提供商的标识，从而认证电子交易的所有证据。

[0019] 根据前述内容，本发明的目的是一种认证电子合同的方法，其特征在于使用第三方认证机构的代理来使用被插入到签署合同方的浏览器中的数字证书验证签署合同方的身份，通过电信运营商或电信提供商(其也可被称为通信提供商或电子通信提供商，这始终是电子交付提供商)认证整个过程。最后，发送方电子通信提供商的客户端接收到合同根据其是否被签署的证书，包括原始电子邮件、合同、日期、时间及其可追溯性、唯一的交易号和CA(认证机构)证书，其中标识数据被包含在浏览器中所包含的数字证书中，其明确地标识签署合同方。

[0020] 本发明的方法可被用于合同及其内容的认证，并且可以使用电子邮件或SMS消息来实现。

附图说明

[0021] 为了补充所作的描述并以帮助更好地理解本发明的特征为目的，根据本发明的优选实际实施例，所述描述作为其整体部分附有一组附图，其中以说明性和非限制性的方式表示了以下内容：

[0022] 图1示出了流程图，其中本发明的方法的一实施例被示为涉及与电子合同相关的电子交易，该过程由发送方实体发起以引入收件人数据和用于验证合同的数据。

[0023] 图2示出了流程图，其中本发明的方法的一实施例被示为涉及与电子合同相关的电子交易，该过程通过经认证SMS或SMS来发起。

[0024] 图3示出了流程图，其中本发明的方法的一实施例被示为涉及与电子合同相关的电子交易，该过程通过经认证电子邮件或电子邮件来发起。

[0025] 发明的优选实施例

[0026] 作为本发明的保护对象的用于电子合同的方法可以在也是本发明的保护对象的

与通信提供商相关联的平台中实现,该平台可由接收方实体和发送方实体以及一系列彼此互连的服务器访问;接收方实体可通过接收者或接收设备(诸如智能电话或接收者的计算机)访问,而发送方实体可通过发送方或发送设备(诸如发送方的计算机或类似设备)访问,所述服务器可以是:

[0027] -被称为Connectaclick服务器的合同服务器,之所以被称为Connectaclick服务器,是因为它是一种实现电子合同系统(诸如以模糊的方式使用电子邮件、web和SMS的电子合同系统)的解决方案。合同服务器被紧密地连接至电信提供商或者作为电信提供商的一部分。

[0028] -被称为Mailcert的电子邮件管理服务器,该服务器允许管理电子邮件并从电子邮件中收集证据,证据可以包括:标题、正文及其附件等等。

[0029] -Mailcert数据库服务器,其存储原始电子邮件的内容,包括标题、正文和附件、与发送相对应的日志部分以及收件人电子邮件服务器的解析信息。其存储历史数据。

[0030] -时间戳或时间戳单元(TSU)服务器,其是由CA提供的在现场实施的时间戳系统,用于对由认证系统生成的证据文档(优选地是PDF)、盖时间戳。该服务器优选地位于电信运营商的基础设施中,但是在某些情况下,如果需要的话,它可以是第三方的实体,并因此物理上位于电信运营商的基础设施的外部。-被称为TSA服务器的证据生成服务器,该服务器生成包括因在合同过程期间汇编证据而产生的所述证据的文档(优选地是PDF格式)。

[0031] -被称为CA确认代理的确认服务器,该服务器通过使用收件人的浏览器中所包含的数字证书来负责确保收件人的身份。

[0032] -经认证消息服务器,其负责从合同的发送方向合同的接收方发送经认证消息(优选地是SMS),在选择通过SMS来执行的情形中是向GSM网络发送经认证消息。

[0033] -经生成文档服务器,其负责大量存储经生成的电子合同证书。

[0034] 作为本发明的第二方面的保护对象的用于认证电子合同的方法具有两个可能的实施例,它们通过使用如图2所示的SMS消息或如图3所示的电子邮件(即经认证SMS或经认证电子邮件(以下称经认证电子邮件))而彼此区分。

[0035] 由此,本发明的第二方面的方法允许执行经认证电子合同的生成,其中(通过电子传送设备(诸如它们的计算机))通过访问数据网络(诸如互联网)来访问合同服务器(Connectaclick服务器)的发送方实体被标识为发送方。

[0036] 一旦用户被认证,要验证的客户端的数据、它们希望执行的电子合同(以下称合同)以及接收者(本文全文中被称为接收者或收件人)的电话号码或电子邮件地址便被引入。对一种类型或其他类型的消息的选择将确定要遵循的步骤以使得:

[0037] -如果电话号码被引入,则SMS将通过经认证SMS服务器被发送,并且过程将利用经认证SMS来被发起。

[0038] -如果电子邮件被引入,则经认证电子邮件将通过Mailcert服务器被发送,并且过程将利用经认证电子邮件来被发起。

[0039] 采用经认证SMS的过程在收件人的接收方电子设备(诸如智能电话)(其具有访问和数据通信能力)接收到消息时被发起,所述消息包含URL(互联网地址),该URL链接到CA服务器的代理服务器,藉此与其余服务器的所有通信被执行。

[0040] 采用经认证SMS的过程继续,收件人访问所述URL,其中CA的代理服务器从接收设

备的浏览器中可能的内容之中请求数字证书,以便被用在交易中。

[0041] 如果其不具有数字证书(该数字证书无效或者其无法访问),则CA的代理服务器结束该过程并示出该过程无法继续,生成名为“CA pdf NOOK”且优选地是PDF格式的不合规文件,其将被存储在经生成PDF服务器上;任选地,来自TSU服务器的时间戳可以被添加到所述不合规文件(CA pdf NOOK)。如果其具有证书,则证书所包含的一系列数据被提取以供其后续验证,类似地且与不合规文件一起发生地使用所述数据生成名为“CA pdf OK”的合规文件,任选地,来自TSU的时间戳可以被添加并且其随后被存储在经生成PDF服务器中。

[0042] 以此方式,当浏览器的证书中所包含的数据与最初引入的数据相匹配时,要签署的合同接着被示出。如果收件人不接受合同(例如拒绝签署),则示出收件人没有接受,过程结束,而如果他们接受合同,则接收者被要求提供收件人的电子邮件地址以发送副本给收件人,并且与收件人的会话结束。

[0043] 一旦与收件人的会话结束,证据生成服务器(TSA服务器)通过编译与互联网上的数据传输、合同本身及其内容、代理CA的经生成PDF以及所使用的操作的任何交易数据相关的所有数据来生成交易的证书。一经生成,所得到的证书便通过时间戳服务器(TSU服务器)用通信提供商的数字签名和时间戳来进行签署。

[0044] 所得到的证书一经加戳,便被发送到负责传送电子邮件的Mailcert服务器,其发送已经签署的合同的证书的两份副本和所有经生成证据,一份发送给发送方实体,而另一份发送给接收方实体,它们将由相应电子邮件服务器接收以便由其各自的用户收集。

[0045] 在其中该方法使用经认证邮件或经认证电子邮件的一些实施例中,该方法是类似的并且在收件人的传入电子邮件服务器接收到初始发送的经认证电子邮件时被发起,其中所述经认证电子邮件可以包含要签署的合同,但是其包含链接到CA的代理服务器的URL(互联网地址),藉此与其余服务器的所有通信被执行。采用经认证电子邮件的过程在收件人、接收者通过其智能电话或计算机访问它们的电子邮件并访问电子邮件中所包括的URL时继续,其中CA代理服务器询问它们智能电话或计算机的浏览器中所包含的什么数字证书将在交易中被使用。如果其没有或不具有对它们的访问权,则代理CA服务器示出该过程无法继续,并以PDF格式生成CA pdf NOOK文件,其将被存储在可向其添加时间戳(TSU)的经生成文档服务器上。如果浏览器具有证书,则其包含的以供其后续验证的数据被提取,利用该数据生成CA pdf OK文件,来自TSU服务器的时间戳可以被添加并且将被存储在经生成PDF服务器上。该过程在用户通过代理CA访问Connectaclick服务器时继续,其中验证浏览器的证书中所包含的数据与最初引入的数据相匹配,并且要签署的合同将被示出。如果收件人不接受,则示出合同没有接受,而过程结束。如果收件人接受合同,则他们被要求提供电子邮件以便发送副本给他们,并且与收件人的会话结束。

[0046] 一旦与收件人的会话结束,证据生成服务器便利用所有互联网数据、合同、代理CA的经生成PDF以及所使用的操作的任何交易数据来准备交易的证书。一经完成,所得到的证书便通过时间戳服务器(TSU服务器)用通信提供商的数字签名和时间戳来签署。所生成的证书被发送到负责传送电子邮件的Mailcert服务器,其发送经签署的合同的证书的两份副本和所有经生成证据,一份发送给发送方实体,而另一份发送给接收方实体,它们将由相应电子邮件服务器接收以便由其各自的用户收集。

[0047] 根据前述内容,本发明的方法目的提供了以下优点:所使用的数字证据和证书能

够来自不同CA或认证实体,在可能的替代实施例中,第二CA(作为代理CA服务器的提供商和第三电子交付提供商,其负责最终包装合同的所有证据、生成合同的整个过程的证书)可以被使用。

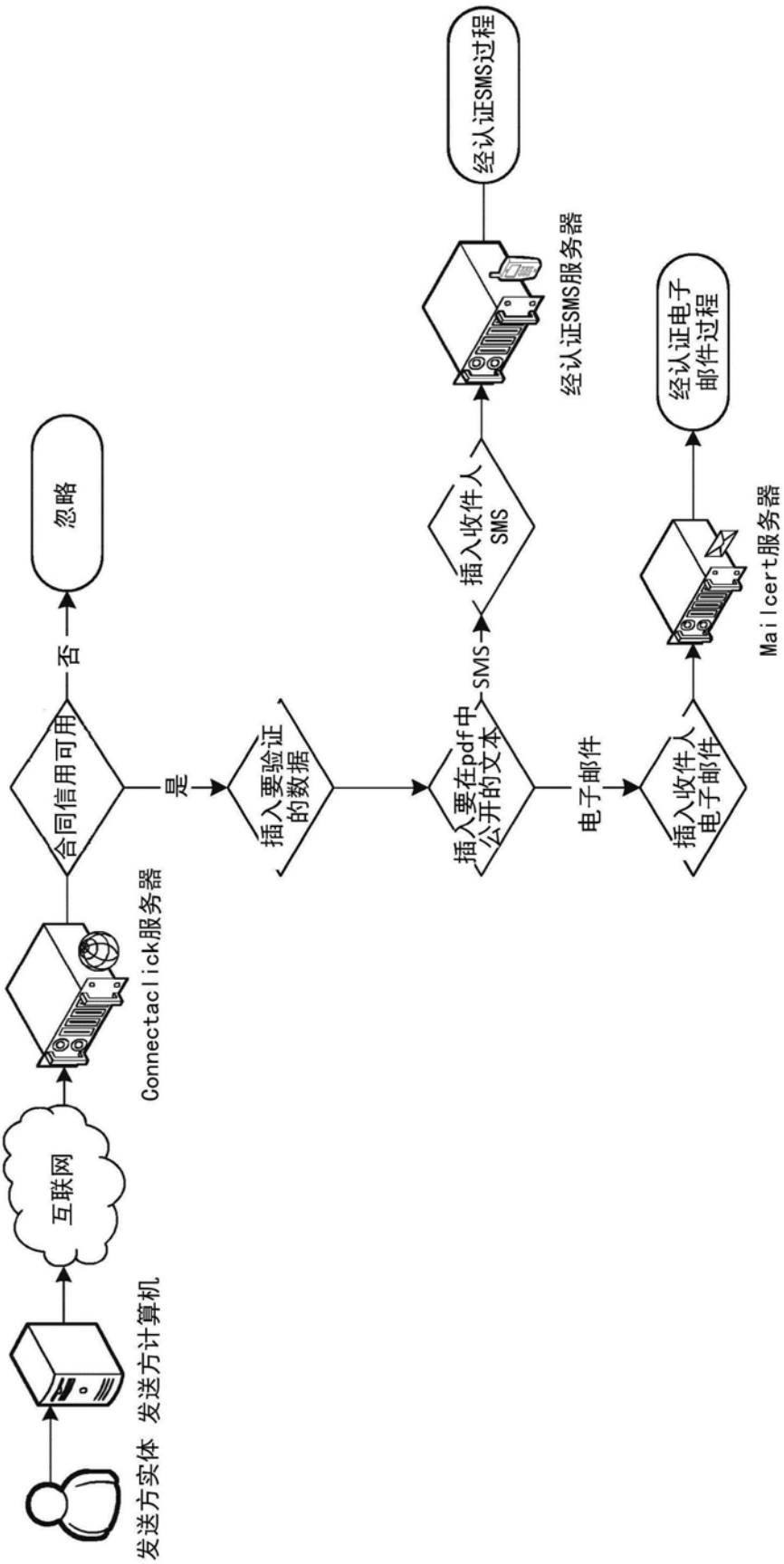

发送方实体
发送方计算机
互联网
Connectaclick服务器
合同信用可用
否
忽略
是
插入要验证的数据
插入要在pdf中公开的文本
SMS
插入收件人SMS
经认证SMS服务器
经认证SMS过程
电子邮件
插入收件人电子邮件
Mailcert服务器
经认证电子邮件过程

图1

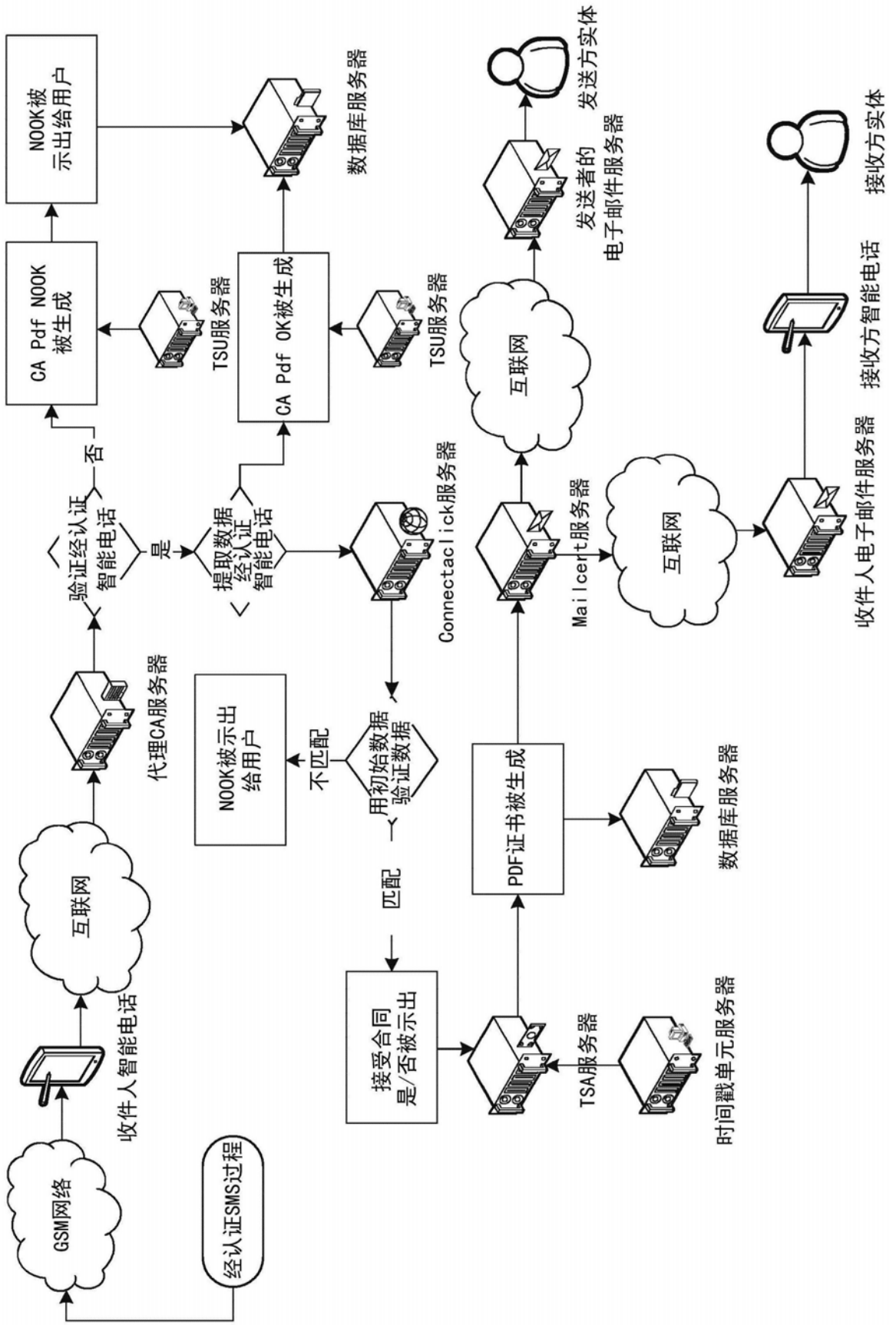

GSM网络
经认证SMS过程
收件人智能电话
互联网
代理CA服务器
验证经认证智能电话
否
是
CA Pdf NOOK被生成
NOOK被示出给用户
TSU服务器
CA Pdf OK被生成
数据库服务器
提取数据经认证智能电话
TSU服务器
Connecticlick服务器
不匹配
NOOK被示出给用户
用初始数据验证数据
匹配
接受合同是/否被示出
TSA服务器
时间戳单元服务器
PDF证书被生成
数据库服务器
互联网
Mailcert服务器
发送者的电子邮件服务器
发送方实体
互联网
收件人电子邮件服务器
接收方智能电话
接收方实体

图2

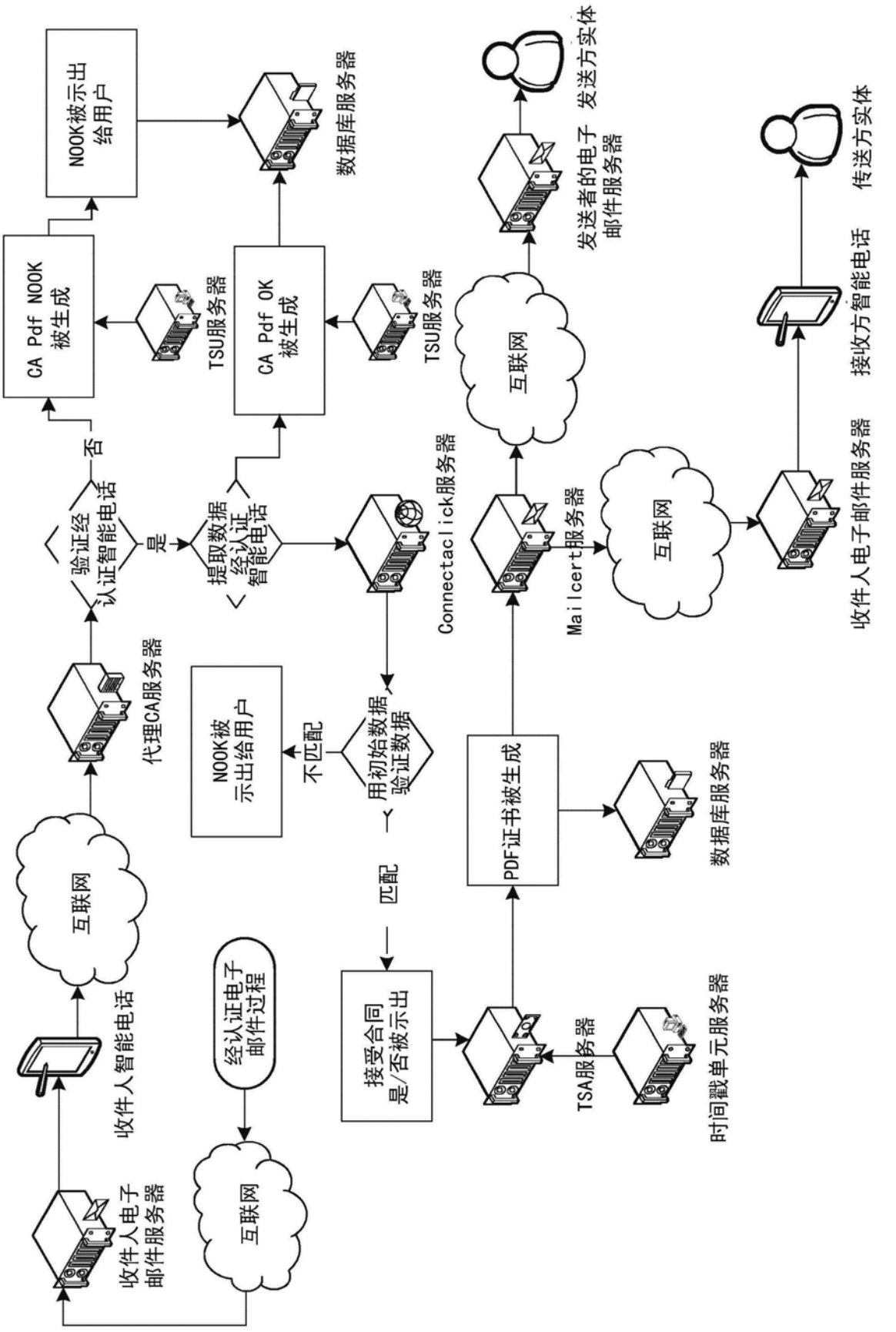

NOOK被示出给用户
数据库服务器
CA Pdf NOOK被生成
TSU服务器
CA Pdf OK被生成
TSU服务器
否
验证经认证智能电话
是
提取数据经认证智能电话
互联网
发送者的电子邮件服务器
发送方实体
代理CA服务器
NOOK被示出给用户
不匹配
用初始数据验证数据
Connectaclick服务器
Mailcert服务器
互联网
收件人电子邮件服务器
接收方智能电话
传送方实体
互联网
收件人智能电话
经认证电子邮件过程
匹配
接受合同是/否被示出
PDF证书被生成
数据库服务器
TSA服务器
时间戳单元服务器
互联网
收件人电子邮件服务器

图3