



(12) 发明专利

(10) 授权公告号 CN 108964925 B

(45) 授权公告日 2020. 11. 24

(21) 申请号 201810978724.1

H04L 29/08 (2006.01)

(22) 申请日 2018.08.27

(56) 对比文件

(65) 同一申请的已公布的文献号

CN 101702150 A, 2010.05.05

申请公布号 CN 108964925 A

CN 101316274 A, 2008.12.03

(43) 申请公布日 2018.12.07

CN 108154351 A, 2018.06.12

(73) 专利权人 胡金钱

CN 103699852 A, 2014.04.02

地址 310008 浙江省杭州市江干区九环路9号4号楼701室

CN 108108611 A, 2018.06.01

US 2005228999 A1, 2005.10.13

审查员 孙铭君

(72) 发明人 胡金钱

(74) 专利代理机构 北京国贝知识产权代理有限公司 11698

代理人 丛芳

(51) Int. Cl.

H04L 9/32 (2006.01)

H04L 29/06 (2006.01)

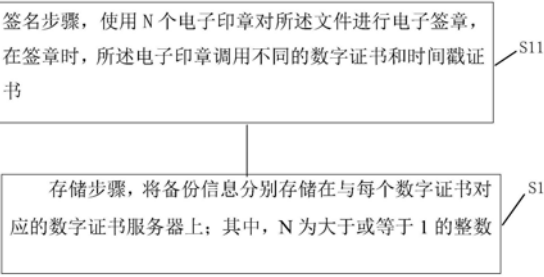
权利要求书3页 说明书8页 附图3页

(54) 发明名称

一种文件认证设备方法、装置、设备及可读介质

(57) 摘要

本发明提供了一种文件认证方法、装置、设备及可读介质,该方法包括:签名步骤,使用N个电子印章对文件进行电子签章,在签章时,所述电子印章调用不同的数字证书和时间戳证书;存储步骤,将备份信息分别存储在与每个数字证书对应的数字证书服务器上。通过将电子签章后N个备份信息进行分布式存储,确保了文件认证的准确性和安全性,且该方法比采用区块链方式进行文件认证资源使用较少,安全性更高。本发明更提出了进行离线电子签章的电子印章设备,其将电子印章和物理印章集成在一起,实现了去中心化,保证了用章安全;并且,当进行认证时,可以调用多个密钥进行交叉验证,增强了电子印章和物理印章的使用的安全性。



1. 一种文件认证方法,其特征在于,该方法包括:

签名步骤,使用N个电子印章对所述文件进行电子签章,在签章时,所述电子印章调用不同的数字证书和时间戳证书;

存储步骤,将备份信息分别存储在与每个数字证书对应的数字证书服务器上;

其中,N为大于或等于1的整数;

所述文件至少盖一个电子印章,每个电子印章使用至少两个数字证书密钥来认证。

2. 根据权利要求1的方法,其特征在于,所述备份信息包括摘要签章信息或原文签章信息,其中,摘要签章信息包括所述文件的摘要信息、签署人的身份信息和时间信息;原文签章信息包括所述文件的全文、签署人的身份信息和时间信息。

3. 根据权利要求2的方法,其特征在于,对所述文件进行电子签章的方式为:用户获取电子印章设备内的智能芯片中存储的至少一个电子印章和至少两个数字证书,并访问数字证书对应的数字证书服务器获取时间戳证书,然后通过所述至少两个数字证书和时间戳证书对所述文件进行电子签章,将所述备份信息发送至对应的数字证书服务器中进行存储。

4. 根据权利要求2的方法,其特征在于,对所述文件进行电子签章的方式为:用户从电子印章服务器中获取至少一个电子印章,然后每个电子印章选择至少两个数字证书服务器中的数字证书以及时间戳证书对所述文件进行电子签章,将所述备份信息存储在对应的数字证书服务器中。

5. 根据权利要求3的方法,其特征在于,所述电子印章设备包括印章壳体,设置在所述印章壳体底部的物理印章,以及容置在所述印章壳体内部且连接所述物理印章的片上系统;

所述片上系统包括:中央控制模块,以及与所述中央控制模块相连接的通讯模块、身份认证模块、密钥模块、存储模块和物理印章模块;

所述通讯模块,用于实现与用户和外部服务器的通讯;

所述身份认证模块,用于存储身份信息,并利用存储的身份信息对用户输入的身份信息进行认证,认证通过后,对用户进行授权;

所述密钥模块,用于存储银行系统和/或政府系统授权的数字证书和密钥;

所述存储模块,用于存储电子印章;

所述中央处理模块,用于在用户获得授权后,从所述存储模块中获取电子印章,并从所述密钥模块获取与所述电子印章对应的至少两个数字证书,访问数字证书对应的数字证书服务器获取时间戳证书,并将所述备份信息发送至对应的数字证书服务器中进行存储;

所述物理印章模块,用于存储物理印章信息,并在接收到批准用户使用物理印章的指令后,控制物理印章动作,提供物理印章给用户使用。

6. 根据权利要求5的方法,其特征在于,所述电子印章设备还包括第一摄像模块,设置在所述印章壳体的顶部,用于获取用户的虹膜信息或面部特征信息并发送给所述身份认证模块进行身份认证;所述物理印章通过可翻转机构设置在所述印章壳体底部,当接收到用户的物理用章请求后并且该请求被批准后,所述物理印章模块控制所述可翻转机构翻转,将所述物理印章的具有章模的一面朝下,提供给用户使用。

7. 根据权利要求6的方法,其特征在于,所述电子印章设备还包括第二摄像模块,设置在所述物理印章上或者可翻转机构上,用于在所述物理印章使用完毕后,将盖章的文件进

行拍照并发送至所述片上系统进行保存。

8. 一种文件认证装置,其特征在於,该装置包括:

签名单元,用于使用N个电子印章对所述文件进行电子签章,在签章时,所述电子印章调用不同的数字证书和时间戳证书备份信息;

存储单元,用于将备份信息分别存储在与每个数字证书对应的数字证书服务器上;

其中,N为大于或等于1的整数;

所述文件至少盖一个电子印章,每个电子印章使用至少两个数字证书密钥来认证。

9. 根据权利要求8的装置,其特征在於,所述备份信息包括摘要签章信息或原文签章信息,其中,摘要签章信息包括所述文件的摘要信息、签署人的身份信息和时间信息;原文签章信息包括所述文件的全文、签署人的身份信息和时间信息。

10. 根据权利要求9的装置,其特征在於,对所述文件进行电子签章的方式为:用户获取电子印章设备内的智能芯片中存储的至少一个电子印章和至少两个数字证书,并访问数字证书对应的数字证书服务器获取时间戳证书,然后通过所述至少两个数字证书和时间戳证书对所述文件进行电子签章备份信息,将所述备份信息发送至对应的数字证书服务器中进行存储。

11. 根据权利要求9的装置,其特征在於,对所述文件进行电子签章的方式为:对所述文件进行电子签章的方式为:用户从电子印章服务器中获取至少一个电子印章,然后每个电子印章选择至少两个数字证书服务器中的数字证书以及时间戳证书对所述文件进行电子签章备份信息,将所述备份信息存储在对应的数字证书服务器中。

12. 根据权利要求10的装置,其特征在於,所述电子印章设备包括印章壳体,设置在所述印章壳体底部的物理印章,以及容置在所述印章壳体内部且连接所述物理印章的片上系统;

所述片上系统包括:中央控制模块,以及与所述中央控制模块相连接的通讯模块、身份认证模块、密钥模块、存储模块和物理印章模块;

所述通讯模块,用于实现与用户和外部服务器的通讯;

所述身份认证模块,用于存储身份信息,并利用存储的身份信息对用户输入的身份信息进行认证,认证通过后,对用户进行授权;

所述密钥模块,用于存储银行系统和/或政府系统授权的数字证书和密钥;

所述存储模块,用于存储电子印章;

所述中央处理模块,用于在用户获得授权后,从所述存储模块中获取电子印章,并从所述密钥模块获取与所述电子印章对应的至少两个数字证书,访问数字证书对应的数字证书服务器获取时间戳证书,并将所述备份信息发送至对应的数字证书服务器中进行存储;

所述物理印章模块,用于存储物理印章信息,并在接收到批准用户使用物理印章的指令后,控制物理印章动作,提供物理印章给用户使用。

13. 根据权利要求12的装置,其特征在於,所述电子印章设备还包括第一摄像模块,设置在所述印章壳体的顶部,用于获取用户的虹膜信息或面部特征信息并发送给所述身份认证模块进行身份认证;所述物理印章通过可翻转机构设置在所述印章壳体底部,当接收到用户的物理用章请求后并且该请求被批准后,所述物理印章模块控制所述可翻转机构翻转,将所述物理印章的具有章模的一面朝下,提供给用户使用。

14. 根据权利要求13的装置,其特征在于,所述电子印章设备还包括第二摄像模块,设置在所述物理印章上或者可翻转机构上,用于在所述物理印章使用完毕后,将盖章的文件进行拍照并发送至所述片上系统进行保存。

15. 一种文件认证设备,其特征在于,所述设备包括处理器、存储器,所述处理器与所述存储器通过总线相连接,所述存储器中存储机器可读代码,所述处理器执行存储器中的机器可读代码以执行权利要求1-7之任一项所述的方法。

16. 一种计算机可读存储介质,其特征在于,所述存储介质上存储有计算机程序代码,当所述计算机程序代码被计算机执行时可执行权利要求1-7之任一的方法。

一种文件认证设备方法、装置、设备及可读介质

技术领域

[0001] 本发明涉及信息安全技术领域,特别是一种文件认证设备方法、装置、设备及可读介质。

背景技术

[0002] 随着互联网技术的快速发展和电子政务、电子商务的兴起,电子印章技术已经应运而生且得到广泛应用。但是,目前的数字证书都是分地域存储的,难以跨地域使用,且目前使用文件在加盖电子印章时一般使用一个数字证书进行签名,若该电子签名被黑客攻破,从而导致电子签名被泄露,影响用户的信息安全性,且使用一个证书进行签名后也无法对文件的真实性进行交叉验证。此外,目前的电子印章与物理印章是分离的,其在使用时,无法做到很好的管控,例如使用前的安全性验证和使用后的查询追踪等。

[0003] 另外,现有技术中采用区块链技术对电子签名后的文件进行多点存储,但是区块链技术复杂,所需资源较多,且每个链节点存储的信息是相同的,这样导致一个节点的信息被攻破,将会泄露所有的用户信息,安全性较低。

发明内容

[0004] 本发明针对上述现有技术中的缺陷,提出了如下技术方案。

[0005] 一种文件认证方法,该方法包括:

[0006] 签名步骤,使用N个电子印章对所述文件进行电子签章,在签章时,所述电子印章调用不同的数字证书和时间戳证书;

[0007] 存储步骤,将备份信息分别存储在与每个数字证书对应的数字证书服务器上;

[0008] 其中,N为大于或等于1的整数。

[0009] 更进一步地,所述文件至少盖一个电子印章,每个电子印章使用至少一个数字证书密钥来认证。

[0010] 更进一步地,所述备份信息包括摘要签章信息或原文签章信息,其中,摘要签章信息包括所述文件的摘要信息、签署人的身份信息和时间信息;原文签章信息包括所述文件的全文、签署人的身份信息和时间信息。

[0011] 更进一步地,对所述文件进行电子签章的方式为:用户获取电子印章设备内的智能芯片中存储的至少一个电子印章和至少一个数字证书,并访问数字证书对应的数字证书服务器获取时间戳证书,然后通过所述至少一个数字证书和时间戳证书对所述文件进行电子签章,将所述备份信息发送至对应的数字证书服务器中进行存储。

[0012] 更进一步地,对所述文件进行电子签章的方式为:用户从电子印章服务器中获取至少一个电子印章,然后每个电子印章选择至少一个数字证书服务器中的数字证书以及时间戳证书对所述文件进行电子签章,将所述备份信息存储在对应的数字证书服务器中。

[0013] 更进一步地,所述电子印章设备包括印章壳体,设置在所述印章壳体底部的物理印章,以及容置在所述印章壳体内部且连接所述物理印章的片上系统;

[0014] 所述片上系统包括：中央控制模块，以及与所述中央控制模块相连接的通讯模块、身份认证模块、密钥模块、存储模块和物理印章模块；

[0015] 所述通讯模块，用于实现与用户和外部服务器的通讯；

[0016] 所述身份认证模块，用于存储身份信息，并利用存储的身份信息对用户输入的身份信息进行认证，认证通过后，对用户进行授权；

[0017] 所述密钥模块，用于存储银行系统和/或政府系统授权的数字证书和密钥；

[0018] 所述存储模块，用于存储电子印章；

[0019] 所述中央处理模块，用于在用户获得授权后，从所述存储模块中获取电子印章，并从所述密钥模块获取与所述电子印章对应的至少一个数字证书，访问数字证书对应的数字证书服务器获取时间戳证书，并将所述备份信息发送至对应的数字证书服务器中进行存储；

[0020] 所述物理印章模块，用于存储物理印章信息，并在接收到批准用户使用物理印章的指令后，控制物理印章动作，提供物理印章给用户使用。

[0021] 更进一步地，所述电子印章设备还包括第一摄像模块，设置在所述印章壳体的顶部，用于获取用户的虹膜信息或面部特征信息并发送给所述身份认证模块进行身份认证；所述物理印章通过可翻转机构设置在所述印章壳体底部，当接收到用户的物理用章请求后并且该请求被批准后，所述物理印章模块控制所述可翻转机构翻转，将所述物理印章的具有章模的一面朝下，提供给用户使用。

[0022] 更进一步地，所述电子印章设备还包括第二摄像模块，设置在所述物理印章上或者可翻转机构上，用于在所述物理印章使用完毕后，将盖章的文件进行拍照并发送至所述片上系统进行保存。

[0023] 本发明还提出了一种文件认证装置，该装置包括：

[0024] 签名单元，用于使用N个电子印章对所述文件进行电子签章，在签章时，所述电子印章调用不同的数字证书和时间戳证书备份信息；

[0025] 存储单元，用于将备份信息分别存储在与每个数字证书对应的数字证书服务器上；

[0026] 其中，N为大于或等于1的整数。

[0027] 更进一步地，所述文件至少盖一个电子印章，每个电子印章使用至少一个数字证书密钥来认证。

[0028] 更进一步地，所述备份信息包括摘要签章信息或原文签章信息，其中，摘要签章信息包括所述文件的摘要信息、签署人的身份信息和时间信息；原文签章信息包括所述文件的全文、签署人的身份信息和时间信息。

[0029] 更进一步地，对所述文件进行电子签章的方式为：用户获取电子印章设备内的智能芯片中存储的至少一个电子印章和至少一个数字证书，并访问数字证书对应的数字证书服务器获取时间戳证书，然后通过所述至少一个数字证书和时间戳证书对所述文件进行电子签章备份信息，将所述备份信息发送至对应的数字证书服务器中进行存储。

[0030] 更进一步地，对所述文件进行电子签章的方式为：对所述文件进行电子签章的方式为：用户从电子印章服务器中获取至少一个电子印章，然后每个电子印章选择至少一个数字证书服务器中的数字证书以及时间戳证书对所述文件进行电子签章备份信息，将所述

备份信息存储在对应的数字证书服务器中。

[0031] 更进一步地,所述电子印章设备包括印章壳体,设置在所述印章壳体底部的物理印章,以及容置在所述印章壳体内部且连接所述物理印章的片上系统;

[0032] 所述片上系统包括:中央控制模块,以及与所述中央控制模块相连接的通讯模块、身份认证模块、密钥模块、存储模块和物理印章模块;

[0033] 所述通讯模块,用于实现与用户和外部服务器的通讯;

[0034] 所述身份认证模块,用于存储身份信息,并利用存储的身份信息对用户输入的身份信息进行认证,认证通过后,对用户进行授权;

[0035] 所述密钥模块,用于存储银行系统和/或政府系统授权的数字证书和密钥;

[0036] 所述存储模块,用于存储电子印章;

[0037] 所述中央处理模块,用于在用户获得授权后,从所述存储模块中获取电子印章,并从所述密钥模块获取与所述电子印章对应的至少一个数字证书,访问数字证书对应的数字证书服务器获取时间戳证书,并将所述备份信息发送至对应的数字证书服务器中进行存储;

[0038] 所述物理印章模块,用于存储物理印章信息,并在接收到批准用户使用物理印章的指令后,控制物理印章动作,提供物理印章给用户使用。

[0039] 更进一步地,所述电子印章设备还包括第一摄像模块,设置在所述印章壳体的顶部,用于获取用户的虹膜信息或面部特征信息并发送给所述身份认证模块进行身份认证;所述物理印章通过可翻转机构设置所述印章壳体底部,当接收到用户的物理用章请求后并且该请求被批准后,所述物理印章模块控制所述可翻转机构翻转,将所述物理印章的具有章模的一面朝下,提供给用户使用。

[0040] 更进一步地,所述电子印章设备还包括第二摄像模块,设置在所述物理印章上或者可翻转机构上,用于在所述物理印章使用完毕后,将盖章的文件进行拍照并发送至所述片上系统进行保存。

[0041] 本发明还提出了一种文件认证设备,所述设备包括处理器、存储器,所述处理器与所述存储器通过总线相连接,所述存储器中存储机器可读代码,所述处理器执行存储器中的机器可读代码以执行上述之任一所述的方法。

[0042] 本发明还提出了一种计算机可读存储介质,所述存储介质上存储有计算机程序代码,当所述计算机程序代码被计算机执行时可执行上述之任一所述的方法。

[0043] 本发明的技术效果为:本发明提出了一种文件认证方法,其使用N个电子印章对所述文件进行电子签章,在签章时,电子印章调用不同的数字证书和时间戳证书,然后将所述N个备份信息分别存储在与每个数字证书对应的数字证书服务器上,其中,N为大于或等于1的整数。通过将电子签章时,调用不同的数字证书,将备份信息分布存储在所调用的不同的数字证书对应的数字证书服务器上,这样,即使某一个数字证书服务器断线或者故障或者损坏,在其他的数字证书服务器中仍保存有备份信息,确保了文件认证的准确性和安全性,且该方法比采用区块链方式进行文件认证资源使用较少,安全性更高。

[0044] 进一步地,本发明更提出了进行离线电子签章的电子印章设备,其将电子印章和物理印章集成在一起,实现了去中心化,保证了用章安全;并且,其中的密钥模块存储了各种银行系统和政府系统的授权证书,当进行认证时,可以调用多个密钥进行交叉验证;在用

章验证时,物理印章模块和电子印章模块可以实现相互交叉验证,增强了电子印章和物理印章的使用的安全性。

附图说明

[0045] 通过阅读参照以下附图所作的对非限制性实施例所作的详细描述,本申请的其它特征、目的和优点将会变得更明显。

[0046] 图1是根据本发明的实施例的一种文件认证方法的流程图。

[0047] 图2是根据本发明的实施例的电子印章设备的结构示意图。

[0048] 图3是根据本发明的实施例的片上系统的结构示意图。

[0049] 图4是根据本发明的实施例的一种文件认证装置的结构示意图。

[0050] 图5是根据本发明的实施例的一种文件认证设备的结构示意图。

具体实施方式

[0051] 下面结合附图和实施例对本申请作进一步的详细说明。可以理解的是,此处所描述的具体实施例仅仅用于解释相关发明,而非对该发明的限定。另外还需要说明的是,为了便于描述,附图中仅示出了与有关发明相关的部分。

[0052] 需要说明的是,在不冲突的情况下,本申请中的实施例及实施例中的特征可以相互组合。下面将参考附图并结合实施例来详细说明本申请。

[0053] 图1示出了本发明的一种文件认证方法,该方法包括:

[0054] 签名步骤S11,使用N个电子印章对所述文件进行电子签章,在签章时,所述电子印章调用不同的数字证书和时间戳证书。

[0055] 在文件认证中,将文件采用一个或者多个电子印章进行电子签章,所述电子印章在签章时,需要访问数字证书服务器调用数字证书和时间戳证书。在调用数字证书和时间戳证书时,将备份信息发送至数字证书服务器并储存在数字证书服务器上。

[0056] 可选地,本实施例中,使用的电子印章为一个时,一个电子印章可以调用两个以上不同的数字证书和时间戳证书,例如浙江数字证书和时间戳证书、北京数字证书和时间戳证书、公安数字证书和时间戳证书等,这样将备份信息发送至不同的数字证书服务器储存。使用的电子印章为多个时,至少有两个电子印章调用不同的数字证书,例如一个电子印章调用浙江数字证书和时间戳证书,一个电子印章调用北京数字证书和时间戳证书;其余的电子印章可调用相同或者不同的数字证书和时间戳证书,这样将备份信息储存至不同的数字证书服务器;较优地,每个电子印章调用的数字证书和时间戳证书都不同,但并不限于此。每个电子印章可以调用一个数字证书和时间戳证书,也可调用两个以上不同的数字证书和时间戳证书;可选择所调用的数字证书和时间戳证书。

[0057] 备份信息为摘要签章信息或原文签章信息,其中,摘要签章信息包括所述文件的摘要信息、签署人的身份信息和时间信息;原文签章信息包括所述文件的全文、签署人的身份信息和时间信息。

[0058] 存储步骤S12,将所述N个备份信息分别存储在与N个数字证书对应的数字证书服务器上;其中,N为大于或等于1的整数。

[0059] 在生成多个电子签章后的备份信息分别存储在与N个数字证书对应的数字证书

(Certification Authority, CA) 服务器上,即每个数字证书服务器存储的都是操作与本地服务器对应的数字证书的备份信息,不会存储与其他数字证书服务器的备份信息。

[0060] 通过将电子签章后至少两个备份信息进行分布式存储,确保了文件认证的准确性和安全性,且该方法采用区块链方式进行文件认证资源使用较少,安全性更高,这是本发明的重要发明点之一。

[0061] 此外,在电子签章后的文件中,至少显示加盖了至少一个电子印章,其中,每个电子印章使用至少一个数字证书密钥来认证,从而提高了文件认证的可靠性。

[0062] 在一个实施例中,用户获取电子印章设备内的智能芯片中存储的至少一个电子印章和至少一个数字证书,并访问数字证书对应的数字证书服务器获取时间戳证书,然后通过所述至少一个数字证书和时间戳证书对所述文件进行电子签章,将所述备份信息发送至对应的数字证书服务器中进行存储。电子印章掌握在客户手中,电子印章具备通信模块,可以与调用电子印章的设备和数字证书服务器进行通信。在电子印章无法与数字证书服务器通信的情况下,电子印章仍然可以依靠存储在电子印章内的数字证书完成离线的签章,这种情况下备份信息可以存储到电子印章的服务器和/或电子印章中。

[0063] 在一个实施例中,对所述文件进行电子签章的方式为:用户从电子印章服务器中获取至少一个电子印章,然后每个电子印章选择至少一个数字证书服务器中的数字证书以及时间戳证书对所述文件进行电子签章,将所述备份信息存储在对应的数字证书服务器中。

[0064] 如图2所示,本发明还提出了用于离线电子签章的一种电子印章设备,所述电子印章设备包括印章壳体,设置在所述印章壳体底部的物理印章,以及容置在所述印章壳体内部且连接所述物理印章的片上系统。

[0065] 如图3所示,所述片上系统包括:中央控制模块31,以及与所述中央控制模块31相连接的通讯模块32、身份认证模块33、密钥模块34、存储模块35和物理印章模块36;所述通讯模块32,用于实现与用户和外部服务器的通讯;所述身份认证模块33,用于存储身份信息,并利用存储的身份信息对用户输入的身份信息进行认证,认证通过后,对用户进行授权;所述密钥模块34,用于存储银行系统和/或政府系统授权的数字证书和密钥;所述存储模块35,用于存储电子印章(包括电子印章的章模、印章编号、使用单位编号、使用单位名称、法人姓名、法人编号等等);所述中央处理模块,用于在用户获得授权后,从所述存储模块35中获取电子印章,并从所述密钥模块34获取与所述电子印章对应的至少一个数字证书,访问数字证书对应的数字证书服务器获取时间戳证书,并将所述备份信息发送至对应的数字证书服务器中进行存储;所述物理印章模块36,用于存储物理印章信息,并在接收到批准用户使用物理印章的指令后,控制物理印章动作,提供物理印章给用户使用。

[0066] 所述物理印章模块36中存储的物理印章信息包括物理印章的章模、印章编号、使用单位编号、使用单位名称、法人姓名、法人编号、印章名称、制作单位编码、制作单位名称、印章类型、材料、制作时间,累计使用次数等等。

[0067] 所述电子印章设备还包括第一摄像模块,设置在所述印章壳体的顶部,用于获取用户的虹膜信息或面部特征信息并发送给所述身份认证模块33进行身份认证;所述物理印章通过可翻转机构设置在所述印章壳体底部,当接收到用户的物理用章请求后并且该请求被批准后,所述物理印章模块36控制所述可翻转机构翻转,将所述物理印章的具有章模的

一面朝下,提供给用户使用。

[0068] 一般说来,片上系统(SoC,也称为系统级芯片),意指它是一个产品,是一个有专用目标的集成电路,其中包含完整系统并有嵌入软件的全部内容。同时它又是一种技术,用以实现从确定系统功能开始,到软/硬件划分,并完成设计的整个过程。从狭义角度讲,它是信息系统核心的芯片集成,是将系统关键部件集成在一块芯片上;从广义角度讲,SoC是一个微小型系统,如果说中央处理器(CPU)是大脑,那么SoC就是包括大脑、心脏、眼睛和手的系统。本发明采用SoC制作电子印章设备,提高了电子印章设备的可靠性和降低了总的系统成本。

[0069] 在一个具体的实施例中,所述物理印章通过可翻转机构设置在该印章壳体底部,当接收到用户的物理用章请求后,用章申请人发送用章请求至服务平台,服务平台将用章请求发送至审批人,审批人同意后,服务平台发送控制指令给电子印章设备,控制印章打开。所述物理印章模块36控制所述可翻转机构翻转,将该物理印章的具有章模的一面朝下,提供给用户使用。

[0070] 所述电子印章设备还包括第二摄像模块,设置在所述物理印章上或者可翻转机构上,用于在所述物理印章使用完毕后,将盖章的文件进行拍照并发送至所述片上系统进行保存。

[0071] 在本实施例中,通讯模块32用于接收用户输入的身份信息和请求指令。当用户为个人用户时,用户输入的身份信息包括用户输入的生物特征信息、网络身份信息或者两者的组合,所述生物特征包括用户输入的指纹信息、虹膜信息以及面部识别信息等,这些信息的输入可通过外部的指纹识别仪、摄像头和面部识别仪器来实现。用户输入的网络身份信息包括个人用户的身份证号、手机号或者用户ID等。用户输入的请求指令,例如可以是用户的用章请求或者用户的查询请求等。

[0072] 另外,通讯模块32还用于实现与外部服务器的通讯。具体实施时,外部服务器包括银行服务器、工商服务器、公安服务器、税务服务器以及其他云服务器(例如用户档案编码服务器)等。通讯模块32可以直接与这些服务器通讯,也可以通过云平台服务器实现与外部服务器的通讯。具体实施时,通讯模块32可以包括3G通讯模块32、4G通讯模块32、5G通讯模块32、WIFI模块、NB-IoT模块、量子通信模块等,利用CDMA、TDSCDMA、CDMA2000、FDD-LTE、TDD-LTE等通讯模式实现与外部的信息交互。

[0073] 密钥模块34中存储银行系统和/或政府系统授权的数字证书和密钥(例如银行密钥、工商密钥、税务密钥、公安密钥、社保密钥、公积金密钥等)以及电子印章的证书等。并且,当文件需要认证时,将所述文件的对应密钥与其他一个或多个密钥进行交叉验证。交叉认证就是例如办理一项公安文件认证时,不需要都在公安的服务器对所有的资料进行重新验证,在需要认证时,可通过查看以前的工商、税务、社保等其他服务器的审批过程,只要材料之前经过其他服务器的审批并核实为真,则在公安服务器处可不再重复进行认证的过程。另外,交叉认证的方式还可以包括在办理一项文件认证时,调用两个以上的密钥进行身份认证,例如:当办理银行业务的文件认证时,不但调用对应的银行密钥进行验证,还调用工商密钥进行同时验证,增强了业务办理的安全性。同理,去工商办事,可以增加身份识别和银行信息的比对,以增强安全性。同时,可以设定不同密钥的调用顺序,以保证更高的安全等级。

[0074] 在接收到批准用户使用印章的指令后,根据所述存储模块35和所述物理印章模块36中分别包含的章模、印章编号、使用单位编号、使用单位名称、法人姓名、法人编号,通过哈希算法,分别生成所述电子印章的编码和物理印章的编码,将得到的编码进行比对,如果相同,则验证通过,授权用户可以用章。通过上述电子印章与所述物理印章的相互验证,一方面增强了用章的安全性,一方面也防止了可能发生的小概率的用章失误。

[0075] 本发明的用于离线电子签章的电子印章设备,其将电子印章和物理印章集成在一起,实现了去中心化,保证了用章安全;并且,其中的密钥模块存储了各种银行系统和政府系统的授权证书,当进行认证时,可以调用多个密钥进行交叉验证;在用章验证时,物理印章模块和电子印章模块可以实现相互交叉验证,增强了电子印章和物理印章的使用的安全性。

[0076] 进一步参考图4,作为对上述图1所示方法的实现,本申请提供了一种操作电子签名的装置的一个实施例,该装置实施例与图1所示的方法实施例相对应,上述对图1中各步骤的详细介绍同样适合于本装置的实施例,该装置具体可以包含于各种电子设备中。

[0077] 如图4所示,本发明还提出了一种文件认证装置,该装置包括:

[0078] 签名单元41,用于使用N个电子印章对所述文件进行电子签章,在签章时,所述电子印章调用不同的数字证书和时间戳证书。

[0079] 在文件认证中,将文件采用一个或者多个电子印章进行电子签章,所述电子印章在签章时,需要访问数字证书服务器调用数字证书和时间戳证书。在调用数字证书和时间戳证书时,将备份信息发送至数字证书服务器并储存在数字证书服务器上。

[0080] 可选地,本实施例中,使用的电子印章为一个时,一个电子印章可以调用两个以上不同的数字证书和时间戳证书,例如浙江数字证书和时间戳证书、北京数字证书和时间戳证书、公安数字证书和时间戳证书等,这样将备份信息发送至不同的数字证书服务器储存。使用的电子印章为多个时,至少有两个电子印章调用不同的数字证书,例如一个电子印章调用浙江数字证书和时间戳证书,一个电子印章调用北京数字证书和时间戳证书;其余的电子印章可调用相同或者不同的数字证书和时间戳证书,这样将备份信息储存至不同的数字证书服务器;较优地,每个电子印章调用的数字证书和时间戳证书都不同,但并不限于此。每个电子印章可以调用一个数字证书和时间戳证书,也可调用两个以上不同的数字证书和时间戳证书;可选择所调用的数字证书和时间戳证书。

[0081] 备份信息为摘要签章信息或原文签章信息,其中,摘要签章信息包括所述文件的摘要信息、签署人的身份信息和时间信息;原文签章信息包括所述文件的全文、签署人的身份信息和时间信息。

[0082] 存储单元42,用于将所述N个备份信息分别存储在与N个数字证书对应的数字证书服务器上;其中,N为大于或等于1的整数。

[0083] 在生成多个电子签章后的备份信息分别存储在与N个电子印章对应的数字证书(CA)服务器上,即每个数字证书服务器存储的都是操作与本地服务器对应的数字证书的备份信息,不会存储与其他数字证书服务器的备份信息。

[0084] 通过将电子签章后至少两个备份信息进行分布式存储,确保了文件认证的准确性和安全性,且该方法采用区块链方式进行文件认证资源使用较少,安全性更高,这是本发明的重要发明点之一。

[0085] 此外,在电子签章后的文件中,至少显示加盖了至少一个电子印章,其中,每个电子印章使用至少一个数字证书密钥来认证,从而提高了文件认证的可靠性。

[0086] 在一个实施例中,

[0087] 用户获取电子印章设备内的智能芯片中存储的至少一个电子印章和至少一个数字证书,并访问数字证书对应的数字证书服务器获取时间戳证书,然后通过所述至少一个数字证书和时间戳证书对所述文件进行电子签章,将所述备份信息发送至对应的数字证书服务器中进行存储。电子印章掌握在客户手中,电子印章具备通信模块,可以与调用电子印章的设备和数字证书服务器进行通信。在电子印章设备无法与数字证书服务器通信的情况下,电子印章设备仍然可以依靠存储在电子印章设备内的数字证书完成盖章,这种情况下备份信息可以存储到电子印章设备的服务器和/或电子印章设备中。

[0088] 在一个实施例中,对所述文件进行电子签章的方式为:用户从电子印章服务器中获取至少一个电子印章,然后每个电子印章选择至少一个数字证书服务器中的数字证书以及时间戳证书对所述文件进行电子签章,将所述备份信息存储在对应的数字证书服务器中。

[0089] 如图4所示的用于离线电子签章的电子印章设备可以是上述图2-3描述的电子印章设备,具体内容如上,在此不再赘述。

[0090] 图5示出了本发明的一种操作电子签名的设备,包括:存储器a和处理器b,所述存储器a中存储计算机程序,所述计算机程序被所述处理器b执行时,所述处理器b执行存储器a中的机器可读代码以执行方法。

[0091] 本发明还提出了一种计算机可读存储介质,所述存储介质上存储有计算机程序代码,当所述计算机程序代码被计算机执行时可执行上述之一的方法。

[0092] 为了描述的方便,描述以上装置时以功能分为各种单元分别描述。当然,在实施本申请时可以把各单元的功能在同一个或多个软件和/或硬件中实现,本发明中所称的客户、客户端指代相同的内容,本发明中的服务端、服务器、服务器端指代相同的内容。

[0093] 通过以上的实施方式的描述可知,本领域的技术人员可以清楚地了解到本申请可借助软件加必需的通用硬件平台的方式来实现。基于这样的理解,本申请的技术方案本质上或者说对现有技术做出贡献的部分可以以软件产品的形式体现出来,该计算机软件产品可以存储在存储介质中,如ROM/RAM、磁碟、光盘等,包括若干指令用以使得一台计算机设备(可以是个人计算机,服务器,或者网络设备等)执行本申请各个实施例或者实施例的某些部分所述的方法。

[0094] 最后所应说明的是:以上实施例仅以说明而非限制本发明的技术方案,尽管参照上述实施例对本发明进行了详细说明,本领域的普通技术人员应当理解:依然可以对本发明进行修改或者等同替换,而不脱离本发明的精神和范围的任何修改或局部替换,其均应涵盖在本发明的权利要求范围当中。

签名步骤，使用 N 个电子印章对所述文件进行电子签章，在签章时，所述电子印章调用不同的数字证书和时间戳证书

S11

存储步骤，将备份信息分别存储在与每个数字证书对应的数字证书服务器上；其中，N 为大于或等于 1 的整数

S12

图1

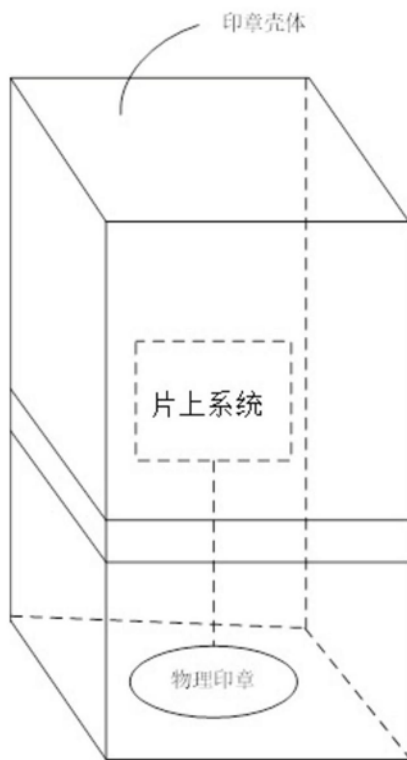


图2

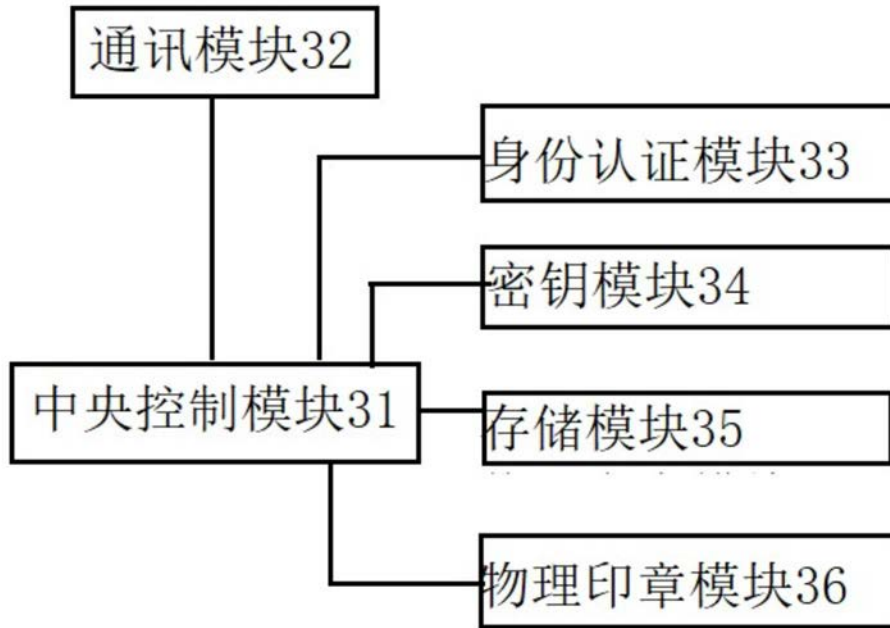


图3



图4

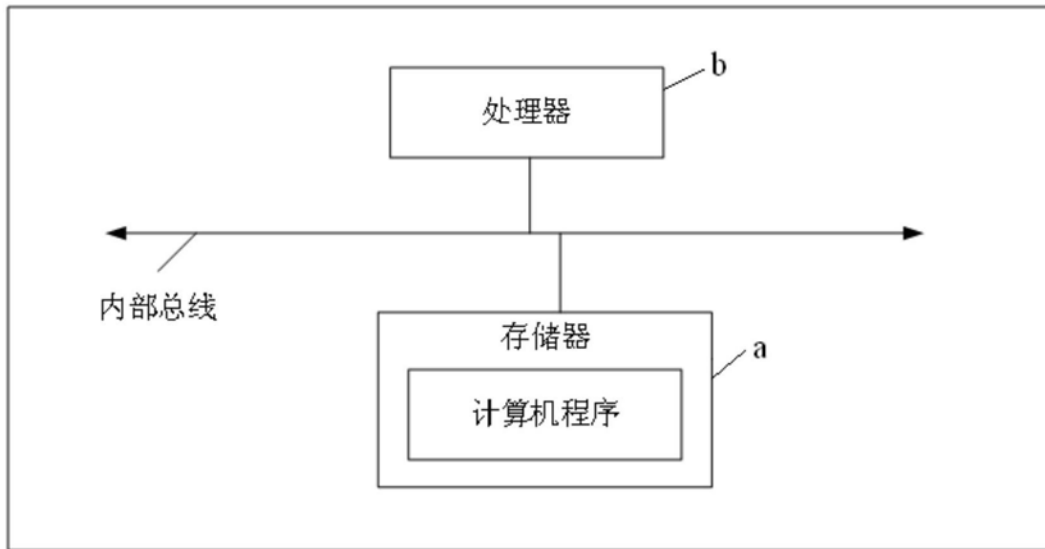


图5