

说明书

发明名称: 基于IPv6的多要素认证根系统及方法

技术领域

[0001] 本发明涉及信息安全技术领域，具体涉及一种根系统及方法。

背景技术

[0002] 根服务器是一款数字信任服务设施，然而传统的根服务器通常需要采用国际数字认证中心认证流程，且往往仅采用单密钥、单证书、单平台认证，只能适合中心化云部属，安全上有疑虑，对于政府、企业、家庭、个人而言并不便利。

[0003] 因此，本领域技术人员亟需研发一种能够有效解决安全疑虑、操作不便等问题的根服务器(即根系统)及方法，来打造从证信、增信、征信到可信的一体化平台，对政府、企业、家庭、个人的数字资产实现全生命周期的管理。

[0004] 应该注意，上面对技术背景的介绍只是为了方便对本发明的技术方案进行清楚、完整的说明，并方便本领域技术人员的理解而阐述的。不能仅仅因为这些方案在本发明的背景技术部分进行了阐述而认为上述技术方案为本领域技术人员所公知。

发明内容

[0005] 为了克服现有技术中的缺陷，本发明实施例提供了一种基于IPv6的多要素认证根系统及方法。

[0006] 本申请实施例公开了一种基于IPv6的多要素认证根系统，包括：第一撮取模块，用于取得用户的复数个身份信息、复数个企业信息和企业码；第二撮取模块，用于取得用户的IPv6数字地址，其中IPv6数字地址包括复数组十六位地址片段；第三撮取模块，用于取得复数个数字认证中心所提供的复数个数字证书和相对应的复数个密钥；信息认证模块，用于根据IPv6数字地址的复数组十六位地址片段对用户的复数个身份信息和复数个企业信息进行数字化认证，并生成复数个已认证身份信息和复数个已认证企业信息；电子名章/公章生成模块，用于根据复数个已认证身份信息和复数个已认证企业信息生成用户的电子名章和电

子公章；根证书签发模块，用于在用户发出根证书签发请求时，通过第三撮取模块链接复数个数字认证中心，根据复数个数字证书和相对应的复数个密钥来对复数个已认证身份信息和复数个已认证企业信息进行多密钥验证，并签发复数个根证书。

- [0007] 进一步地，电子名章为印刷版电子姓名图章或手写电子姓名图章，可选地，电子名章还需要进行手写签名。
- [0008] 进一步地，该根系统还包括：绑定模块，用于将企业码与IPv6数字地址进行绑定，并生成基于IPv6的域名。
- [0009] 进一步地，企业码是以固定电话号码进行绑定，且固定电话号码是符合全球性金融安全级别的数字化应用。
- [0010] 进一步地，基于IPv6的多要素认证根系统是全球全局性数字化应用的证密链操作系统。
- [0011] 进一步地，该根系统还包括：笔画数字化模块，用于根据笔画数字代码表将复数个身份信息中的每一个中文文字转换成一组数字代码。
- [0012] 进一步地，该根系统还包括多模块。多模块包括：中央控制模块，以及与中央控制模块相连接的通信模块、身份认证模块、密钥模块以及存储模块；通信模块，用于实现基于IPv6的多要素认证根系统与外部服务器的通信；身份认证模块，用于对用户输入的生物识别数据进行认证以生成已认证生物识别数据，并于认证通过后，对用户进行授权；密钥模块，用于存储复数个密钥，并根据复数个密钥中相对应的密钥来对复数个已认证身份信息和复数个已认证企业信息进行加密，以生成复数个加密的已认证身份信息和复数个加密的已认证企业信息；存储模块，用于存储已认证生物识别数据、复数个加密的已认证身份信息、复数个加密的已认证企业信息、电子名章、电子公章和复数个根证书；以及中央控制模块，用于接收输入并控制其他模块的操作，并在用户获得授权后，允许用户调用电子名章和电子公章。
- [0013] 本申请实施例还公开了一种基于IPv6的多要素根认证方法，该方法包括以下步骤：提供基于IPv6的多要素认证根系统，基于IPv6的多要素认证根系统包括第一撮取模块、第二撮取模块、第三撮取模块、信息认证模块、电子名章/公章生

成模块以及根证书签发模块；利用第一撮取模块，来取得用户的复数个身份信息、复数个企业信息和企业码；利用第二撮取模块，来取得用户的IPv6数字地址，其中IPv6数字地址包括复数组十六位地址片段；利用第三撮取模块，来取得复数个数字认证中心所提供的复数个数字证书和相对应的复数个密钥；利用信息认证模块，来根据IPv6数字地址的复数组十六位地址片段对用户的复数个身份信息和复数个企业信息进行数字化认证，并生成复数个已认证身份信息和复数个已认证企业信息；利用电子名章/公章生成模块，来根据用户的复数个已认证身份信息和复数个已认证企业信息来生成用户的电子名章和电子公章；利用根证书签发模块，来在用户发出根证书签发请求时，通过第三撮取模块链接复数个数字认证中心，根据复数个数字证书和相对应的复数个密钥来对复数个已认证身份信息和复数个已认证企业信息进行多密钥验证，并签发复数个根证书。

[0014] 借由以上的技术方案，本发明的有益效果如下：与现有技术相比较，本发明提供的基于IPv6的多要素认证根系统和方法，其优点包括：(1)在基于IPv6协议的基础上，通过集约多个可信要素到数字认证中心数字认证同等安全的证书，本发明的系统不但能够实现IPv6与IPv4双栈互通，同时还能够实现所有数字认证中心数字认证及全国电子印章认证的多类别互通互认；(2)能够在单一平台上一次认证完成多证书、多密钥申请签发；能够写入多种最安全存储介质设备；(3)通过证密链管理，创新性地完成实体从“诞生”初始，就有了多要素、多证照的认证并存储，通过一号多用建立一主多副、一户多密分发运行模式；(4)本发明的数字认证独立于国际CA认证体系，安全可靠。除此之外，本发明的基于IPv6的多要素认证根系统和方法还可通过笔画数字代码表将每一个中文文字转换成一组数字代码D_Code，使计算机可读取，进一步从底层开始将书写代码语言中国化，使得书写代码语言不再局限于西方的英文。换句话说，本发明的基于IPv6的多要素认证根系统是一款中国自有知识产权的数字信任服务设施，它基于新一代IPv6数字地址认证为基础，同时集约企业与个人全局多要素认证为核心，融合国内与国际数字认证中心认证互信服务，形成统一集约、多密钥、多要素、企业与个人信用体系的稳固底座。

[0015] 为了让本发明的上述和其他目的、特征和优点能更明显易懂，下文列举较佳实施例，并结合附图，作详细说明如下。

附图说明

[0016] 为了更清楚地说明本发明实施例或现有技术中的技术方案，下面将对实施例或现有技术描述中所需要使用的附图作简单的介绍，显而易见地，下面描述中的附图仅仅是本发明的一些实施例，对于本领域普通技术人员而言，在不付出创造性劳动的前提下，还可以根据这些附图获得其他的附图。

[0017] 图1是本发明第一实施例中的一种基于IPv6的多要素认证根系统的框架图。

[0018] 图2是本发明第二实施例中的一种基于IPv6的多要素认证根系统的框架图。

[0019] 图3是本发明第三实施例中的一种基于IPv6的多要素认证根系统的框架图。

[0020] 图4是本发明的笔画数字代码表的一实施例的示意图。

[0021] 图5是图1、图2、图3中的多模块的框架图。

[0022] 图6是本发明第一实施例中的一种基于IPv6的多要素根认证方法的流程图。

[0023] 图7是本发明第二实施例中的一种基于IPv6的多要素根认证方法的流程图。

[0024] 以上附图的附图标记：

[0025] 10A、10B、10C基于IPv6的多要素认证根系统

[0026] 110第一撷取模块

[0027] 120第二撷取模块

[0028] 130第二撷取模块

[0029] 140信息认证模块

[0030] 150电子名章/公章生成模块

[0031] 160根证书签发模块

[0032] 170绑定模块

[0033] 180笔画数字化模块

[0034] 200多模块

[0035] 30A-30N数字认证中心

[0036] 210中央控制模块

[0037] 220通信模块

- [0038] 230身份认证模块
- [0039] 240密钥模块
- [0040] 250存储模块
- [0041] ID1-IDn身份信息
- [0042] aID1-aIDn已认证身份信息
- [0043] eaID1-eaIDn加密的已认证身份信息
- [0044] CI1-CIm企业信息
- [0045] aCI1-aCIm已认证企业信息
- [0046] eaCI1-eaCIm加密的已认证企业信息
- [0047] Code_E企业码
- [0048] IPv6_ADDIPv6数字地址
- [0049] ADD_S1-ADD_Sq十六位地址片段
- [0050] CAC1-CACp数字证书
- [0051] KEY1-KEYp密钥
- [0052] EPS电子名章
- [0053] ECS电子公章
- [0054] REQ根证书签发请求
- [0055] ROOT_C1-ROOT_Cq根证书
- [0056] ROOT_DN域名
- [0057] D_Code数字代码
- [0058] BID生物识别数据
- [0059] aBID已认证生物识别数据
- [0060] S610-S670、S710-S760步骤

具体实施方式

- [0061] 下面将结合本发明实施例中的附图，对本发明实施例中的技术方案进行清楚、完整地描述，显然，所描述的实施例仅仅是本发明一部分实施例，而不是全部的实施例。基于本发明中的实施例，本领域普通技术人员在没有做出创造性劳动前提下所获得的所有其他实施例，都属于本发明保护的范围。

- [0062] 需要说明的是，在本发明的描述中，术语“第一”、“第二”等仅用于描述目的和区别类似的对象，两者之间并不存在先后顺序，也不能理解为指示或暗示相对重要性。此外，在本发明的描述中，除非另有说明，“多个”的含义是两个或两个以上。
- [0063] 请参考图1，图1是本发明第一实施例中的一种基于IPv6的多要素认证根系统10A的框架图。如图1所示，基于IPv6的多要素认证根系统10A包括第一撮取模块110、第二撮取模块120、第三撮取模块130、信息认证模块140、电子名章/公章生成模块150、根证书签发模块160以及多模块200。第一撮取模块110用于取得用户的复数个身份信息ID1-IDn、复数个企业信息CI1-CIm和企业码Code_E。第二撮取模块120用于取得用户的IPv6数字地址IPv6_ADD，其中IPv6数字地址IPv6_ADD包括复数组十六位地址片段ADD_S1-ADD_Sq。第三撮取模块130用于取得复数个数字认证中心(Certificate Authority)30A-30N所提供的复数个数字证书CAC1-CACp和相对应的复数个密钥KEY1-KEYp。信息认证模块140耦接于第一撮取模块110、第二撮取模块120和第三撮取模块130，用于根据IPv6数字地址IPv6_ADD的复数组十六位地址片段ADD_S1-ADD_Sq对用户的复数个身份信息ID1-IDn和复数个企业信息CI1-CIm进行实体或数字化认证，并生成复数个已认证身份信息aID1-aIDn和复数个已认证企业信息aCI1-aCIm。电子名章/公章生成模块150耦接于信息认证模块140，用于根据用户的复数个已认证身份信息aID1-aIDn和复数个已认证企业信息aCI1-aCIm来生成用户的电子名章EPS和电子公章ECs。根证书签发模块160耦接于信息认证模块140，用于在用户发出根证书签发请求REQ时，通过第三撮取模块130链接复数个数字认证中心30A-30N，根据复数个数字证书CAC1-CACp和相对应的复数个密钥KEY1-KEYp来对复数个已认证身份信息aID1-aIDn和复数个已认证企业信息aCI1-aCIm进行多密钥验证，并签发复数个根证书ROOT_C1-ROOT_Cq。
- [0064] 请注意，复数个身份信息ID1-IDn可包括用户的公司开设人的身份证、银行账号、地址、邮箱号、绑定移动电话号码、绑定固定电话号码、微信账号、支付宝账号、京东账号、拼多多账号、微博号、QQ号、抖音号、直播间号和/或视频号等，而复数个企业信息CI1-CIm可包括银行系统和/或政府系统授权企业用

户的绑定固定电话号码、绑定银行账号、电子营业执照、税控信息、公章号、法人证件号、统一社会信用代码、电子证照号、企业微信号、直播间号和/或视频号等，但仅为示例说明，本发明并不局限于此。

- [0065] 电子名章为印刷版电子姓名图章或手写电子姓名图章，可选地，电子名章还需要进行手写签名。
- [0066] 请注意，企业码Code_E是以固定电话号码进行绑定，且固定电话号码是符合全球性金融安全级别的数字化应用。因此，本发明的基于IPv6的多要素认证根系统10A/10B/10C是一个全球全局性数字化应用的证密链操作系统。
- [0067] 请参考图2，图2是本发明第二实施例中的一种基于IPv6的多要素认证根系统10B的框架图。图2的基于IPv6的多要素认证根系统10B与图1的基于IPv6的多要素认证根系统10A架构类似，两者差异之处在于图2的基于IPv6的多要素认证根系统10B还包括绑定模块170，耦接于第一撷取模块110和第二撷取模块120，用于将企业码Code_E与IPv6数字地址IPv6_ADD进行绑定，并生成基于IPv6的域名ROOT_DN。
- [0068] 基于IPv6的域名ROOT_DN可以是一个基于IPv6协议来定义的域名，例如：以基于中国的根域名“.ipv6”结尾以区别于现有已存在的基于境外的根域名“.com”、“.net”等。在将企业码Code_E与IPv6数字地址IPv6_ADD进行绑定后可生成基于IPv6的域名ROOT_DN，例如“059188881234.ipv6”、“059188881234.cn.ipv6”等。
- [0069] 请参考图3，图3是本发明第三实施例中的一种基于IPv6的多要素认证根系统10C的框架图。图3的基于IPv6的多要素认证根系统10C与图2的基于IPv6的多要素认证根系统10B架构类似，两者差异之处在于图3的基于IPv6的多要素认证根系统10C还包括笔画数字化模块180，耦接于第一撷取模块110，用于根据笔画数字代码表将复数个身份信息ID1-IDn中的每一个中文文字转换成一组数字代码D_Code。
- [0070] 请参考图4，图4是本发明的笔画数字代码表的一实施例的示意图。笔画通常是指组成汉字且不间断的各种形状的点 and 线，如横(一)、竖(丨)、撇(丿)、点(丶)、捺(㇏)等，笔画是构成汉字字形的最小连笔单位。图4将常用的汉字笔画以及相

对应的数字代码D_Code整理出来，总共分为三十二种笔画，例如，笔画横(一)对应到的数字代码D_Code为“01”，笔画竖(丨)对应到的数字代码D_Code为“02”，笔画撇(丿)对应到的数字代码D_Code为“03”，……，笔画横折折折钩(乛)对应到的数字代码D_Code为“32”，以此类推。如此一来，笔画数字化模块180便能够根据图4中的笔画数字代码表将复数个身份信息ID1-IDn中的每一个中文文字转换成一组数字代码D_Code。举例来说，身份信息包括姓名信息，如“古今”，其中“古”按照书写顺序可依序拆解成笔画横(一)、笔画撇(丿)、笔画竖(丨)、笔画横折(乚)、笔画横(一)五个笔画，因此“古”经过转化后生成的数字代码D_Code为(01, 03, 02, 09, 01)；“今”按照书写顺序可依序拆解成笔画撇(丿)、笔画捺(㇏)、笔画点(丶)、笔画横撇(㇇)四个笔画，因此“今”经过转化后生成的数字代码D_Code为(03, 05, 04, 07)。并且可选地，D_Code可以在末尾包含序列码，以区别笔画及书写顺序相同的文字。例如，“土”按照书写顺序可依序拆解成笔画横(一)、笔画竖(丨)、笔画横(一)三个笔画，“土”经过转化后生成的数字代码D_Code为(01, 02, 01, 1)，数字代码D_Code的末尾“1”为序列码；“士”按照书写顺序可依序拆解成笔画横(一)、笔画竖(丨)、笔画横(一)三个笔画，“士”经过转化后生成的数字代码D_Code为(01, 02, 01, 2)，数字代码D_Code的末尾“2”为序列码。

[0071] 请注意，在特定的情况下，上述的第三撷取模块130也是可以省略的，其功能可由第二撷取模块120来取代。换句话说，本发明的基于IPv6的多要素认证根系统10A/10B/10C可以利用IPv6数字地址IPv6_ADD来代替数字证书进行认证，加上笔画数字化模块180可通过如图4的笔画数字代码表将每一个中文文字转换成一组数字代码D_Code，使计算机可读取，进一步从底层开始将书写代码语言中国化。

[0072] 请一并参考图1至图3和图5，图1至图3中的基于IPv6的多要素认证根系统10A/10B/10C还包括多模块200。如图5所示，多模块200包括中央控制模块210，以及与中央控制模块210相连接的通信模块220、身份认证模块230、密钥模块240以及存储模块250。通信模块220用于实现基于IPv6的多要素认证根系统10A/10B/10C与外部服务器的通信。身份认证模块230，用于对用户输入的生物识别数据B

ID进行认证以生成已认证生物识别数据aBID，并于认证通过后，对用户进行授权。密钥模块240，用于存储复数个密钥KEY1-KEYp，并根据复数个密钥KEY1-KEYp中相对应的密钥来对复数个已认证身份信息aID1-aIDn和复数个已认证企业信息aCI1-aCIIm进行加密，以生成复数个加密的已认证身份信息eaID1-eaIDn和复数个加密的已认证企业信息eaCI1-eaCIIm。存储模块250，用于存储已认证生物识别数据aBID、复数个加密的已认证身份信息eaID1-eaIDn、复数个加密的已认证企业信息eaCI1-eaCIIm、电子名章EPS、电子公章ECS和复数个根证书ROOT_C1-ROOT_Cq。中央控制模块210，用于接收输入并控制其他模块220-250的操作，并在用户获得授权后，允许用户调用电子名章EPS和电子公章ECS。

[0073] 一般来说，上述的电子名章是指经过授权认证后具有印章、印鉴的数字图像，电子签名则是在触摸屏、手写板、计算机、平板或手机上进行手写签名。

[0074] 此外，无论是中文、英文或是其他语言，都可以将姓氏与名字以最小单元的每一个字(词)分开来制作认证授权应用，也就是说，在本发明中，单平台无法签一个完整的姓名。举例来说，“古今来”就需要由三个不同的平台来分别对“古”、“今”、“来”进行认证授权应用。而经过认证授权之后的电子名章/电子签名也需要与手机号码和/或邮箱号进行绑定，做一体化的使用。

[0075] 进一步地，通信模块220可包括：3G通信模块、4G通信模块、5G通信模块、WIFI模块、NBIoT模块、蓝牙模块、NFC模块和红外模块中的至少一种；通信模块220支持IPv4和IPv6协议。

[0076] 请注意，此处的电子名章EPS可以是一个跨域电子名章或者跨域电子签名或者涵盖两者，电子名章为印刷版电子姓名图章或手写电子姓名图章，电子名章的语言可以是世界各国的语言，所对应的号就是绑定的手机号码。可选地，电子名章还需要进行手写电子签名，电子签名的语言可以是世界各国的语言，所对应的号就是绑定的手机号码。

[0077] 请注意，上述的生物识别数据BID可包括指纹信息数据、掌纹信息数据、虹膜信息数据、面部特征识别数据、声纹信息数据和/或心电图数据，或者任何可识别用户的生物特征数据。在实际的应用中，可采取其中一种或者多种的组合来进行安全辨识。此外，在利用生物特征数据BID进行认证的过程中，需要注重

生理(Physical)特征与行为(Behavioral)特征,生理特征包含指纹、掌纹、掌型、虹膜、面容、声纹、DNA等,行为特征则有姿势、心跳、签名等。

[0078] 值得注意的是,本发明的基于IPv6的多要素认证根系统不但是一个基于IPv6基础的多要素认证的根服务器,同时也是一个基于中文笔划书写应用数字化服务器。在基于IPv6协议的基础上,通过集约多个可信要素到数字认证同等安全的证书,本发明的集证通系统不但能够实现IPv6与IPv4双栈互通,同时还能够实现所有数字认证及全国电子印章认证的多类别互通互认;并且,本发明的数字认证独立于国际CA认证体系,安全可靠。此外,通过如图4的笔画数字代码表将每一个中文文字转换成一组数字代码D_Code,使计算机可读取,进一步从底层开始将书写代码语言中国化,使得书写代码语言不再局限于西方的英文。换句话说,本发明的基于IPv6的多要素认证根系统是一款中国自有知识产权的数字信任服务设施,它基于新一代IPv6数字地址认证为基础,同时以集约企业与个人全局多要素认证为核心,融合国内与国际数字认证互信服务,形成统一集约、多密钥、多要素、企业与个人信用体系的稳固底座。

[0079] 请再注意,对于除个人以外的任何单位或机构而言,本发明的基于IPv6的多要素认证根系统皆是以绑定固定电话号码作唯一的数字记号,数据的每个要素都带着固定电话号码作为一个重要认证要素;而对于个人和家庭而言,本发明的基于IPv6的多要素认证根系统则需要匹配与绑定实名认证的手机号码。

[0080] 本发明的基于IPv6的多要素认证根系统可以是一个可信认证的服务器系统,或者一个第三方认证平台系统,这个终端装置包括电子印章等各种证书密钥的认证、存储、管理、应用,它对应的是社会经济交易任何一个部门或者平台系统,包括政府、企业、个人、家庭。

[0081] 本发明的基于IPv6的多要素认证根系统可由一个物电一体智能电子印章的芯片来实现,物电一体智能电子印章的芯片存储各种证书和密钥,所有证书和密钥都可以进行远程分发、下载、存储、应用。

[0082] 请一并参考图1和图6,图6是本发明第一实施例中的一种基于IPv6的多要素根认证方法的流程图。图6中的基于IPv6的多要素根认证方法包括以下步骤:

- [0083] 步骤S610: 提供基于IPv6的多要素认证根系统, 基于IPv6的多要素认证根系统包括第一撮取模块、第二撮取模块、第三撮取模块、信息认证模块、电子名章/公章生成模块以及根证书签发模块;
- [0084] 步骤S620: 利用第一撮取模块, 来取得用户的复数个身份信息、复数个企业信息和企业码;
- [0085] 步骤S630: 利用第二撮取模块, 来取得用户的IPv6数字地址, 其中IPv6数字地址包括复数组十六位地址片段;
- [0086] 步骤S640: 利用第三撮取模块, 来取得复数个数字认证中心所提供的复数个数字证书和相对应的复数个密钥;
- [0087] 步骤S650: 利用信息认证模块, 来根据IPv6数字地址的复数组十六位地址片段对用户的复数个身份信息和复数个企业信息进行实体或数字化认证, 并生成复数个已认证身份信息和复数个已认证企业信息;
- [0088] 步骤S660: 利用电子名章/公章生成模块, 来根据用户的复数个已认证身份信息和复数个已认证企业信息来生成用户的电子名章和电子公章;
- [0089] 步骤S670: 利用根证书签发模块, 来在用户发出根证书签发请求时, 通过第三撮取模块链接复数个数字认证中心, 根据复数个数字证书和相对应的复数个密钥来对复数个已认证身份信息和复数个已认证 ([0090] 请注意, 步骤S620是由第一撮取模块110所执行, 步骤S630是由第二撮取模块120所执行, 步骤S640是由第三撮取模块130所执行, 步骤S650是由信息认证模块140所执行, 步骤S660是由电子名章/公章生成模块150所执行, 步骤S670是由根证书签发模块160所执行。
- [0091] 请一并参考图5和图7, 图7是本发明第二实施例中的一种基于IPv6的多要素根认证方法的流程图。图7中的基于IPv6的多要素根认证方法包括以下步骤:
- [0092] 步骤S710: 提供中央控制模块, 以及与中央控制模块相连接的通信模块、身份认证模块、密钥模块以及存储模块;
- [0093] 步骤S720: 利用通信模块, 来实现基于IPv6的多要素认证根系统与外部服务器的通信;

- [0094] 步骤S730：利用身份认证模块，来对用户输入的生物识别数据进行认证以生成已认证生物识别数据，并于认证通过后，对用户进行授权；
- [0095] 步骤S740：利用密钥模块，来存储复数个密钥，并根据复数个密钥中相对应的密钥来对复数个已认证身份信息和复数个已认证企业信息进行加密，以生成复数个加密的已认证身份信息和复数个加密的已认证企业信息；
- [0096] 步骤S750：利用存储模块，来存储已认证生物识别数据、复数个加密的已认证身份信息、复数个加密的已认证企业信息、电子名章、电子公章和复数个根证书；以及
- [0097] 步骤S760：利用中央控制模块来接收输入并控制其他模块的操作，并在用户获得授权后，允许用户调用电子名章和电子公章。
- [0098] 请注意，步骤S720是由通信模块220所执行，步骤S730是由身份认证模块230所执行，步骤S740是由密钥模块240所执行，步骤S750是由存储模块250所执行，步骤S760是由中央控制模块210所执行。
- [0099] 本发明具体实施例提供一种基于IPv6的多要素认证根系统和方法，能够以多证书、多密钥、多要素、多平台来对根证书进行签发，因此相较于传统根系统仅支持单证书、单密钥、单要素、单平台，本发明能够有效解决安全疑虑、操作不便等问题。再者，本发明的基于IPv6的多要素认证根系统以物电一体应用来进行私有化部署，且每个智能终端都是一个集成算力、存储的边缘云，智能终端包括集证通征信服务器、智能印章、集证通机顶盒、集证通路由器、集证U盾等，因此能够解决私钥中心化部署不安全问题。此外，本发明的基于IPv6的多要素认证根系统绑定固定电话号码和/或手机号码，能够实现一号多用拓展数字空间，打造从证信、增信、征信到可信的一体化平台，对政府、企业、家庭、个人的数字资产实现全生命周期的管理。
- [0100] 上述的本发明实施例可在各种硬件、软件编码或两者组合中进行实施。例如，本发明的实施例也可在数据信号处理器(Digital Signal Processor, DSP)中执行上述方法的程序代码。本发明也可涉及计算机处理器、数字信号处理器、微处理器或现场可编程门阵列(Field Programmable Gate Array, FPGA)执行的多种功能。可根据本发明配置上述处理器执行特定任务，其通过执行定义了本发明揭示的

特定方法的机器可读软件代码或固件代码来完成。可将软件代码或固件代码发展为不同的程序语言与不同的格式或形式。也可为不同的目标平台编译软件代码。然而，根据本发明执行任务的软件代码与其他类型配置代码的不同代码样式、类型与语言不脱离本发明的精神与范围。

[0101] 借由以上的技术方案，本发明的有益效果如下：与现有技术相比较，本发明提供的基于IPv6的多要素认证根系统和方法，其优点包括：(1)在基于IPv6协议的基础上，通过集约多个可信要素到数字认证同等安全的证书，本发明的系统不但能够实现IPv6与IPv4双栈互通的同时，还能够实现所有数字认证及全国电子印章认证的多类别互通互认；(2)能够在单一平台上一次认证完成多证书、多密钥申请签发；能够写入多种最安全存储介质设备；(3)通过证密链管理，创新性地完成实体从“诞生”初始，就有了多要素、多证照的认证并存储，通过一号多用建立一主多副、一户多密分发运行模式；(4)本发明的数字认证独立于国际CA认证体系，安全可靠。除此之外，本发明的基于IPv6的多要素认证根系统和方法还可通过笔画数字代码表将每一个中文文字转换成一组数字代码D_Code，使计算机可读取，进一步从底层开始将书写代码语言中国化，使得书写代码语言不再局限于西方的英文。换句话说，本发明的基于IPv6的多要素认证根系统是一款中国自有知识产权的数字信任服务设施，它基于新一代IPv6数字地址认证为基础，同时集约企业与个人全局多要素认证为核心，融合国内与国际数字认证中心认证互信服务，形成统一集约、多密钥、多要素、企业与个人信用体系的稳固底座。

[0102] 本发明中应用了具体实施例对本发明的原理及实施方式进行了阐述，以上实施例的说明只是用于帮助理解本发明的方法及其核心思想；同时，对于本领域的普通技术人员，依据本发明的思想，在具体实施方式及应用范围上均会有改变之处，综上，本说明书内容不应理解为对本发明的限制。

权利要求书

[权利要求 1]

一种基于IPv6的多要素认证根系统，包括：

第一摄取模块，用于取得用户的复数个身份信息、复数个企业信息和企业码；

第二摄取模块，用于取得所述用户的IPv6数字地址，其中所述IPv6数字地址包括复数组十六位地址片段；

第三摄取模块，用于取得复数个数字认证中心所提供的复数个数字证书和相对应的复数个密钥；

信息认证模块，耦接于所述第一摄取模块、所述第二摄取模块和所述第三摄取模块，用于根据所述IPv6数字地址的所述复数组十六位地址片段对所述用户的所述复数个身份信息和所述复数个企业信息进行实体或数字化认证，并生成复数个已认证身份信息和复数个已认证企业信息；

电子名章/公章生成模块，耦接于所述信息认证模块，用于根据所述复数个已认证身份信息和所述复数个已认证企业信息生成所述用户的电子名章和电子公章；

根证书签发模块，耦接于所述信息认证模块，用于在所述用户发出根证书签发请求时，通过所述第三摄取模块链接所述复数个数字认证中心，根据所述复数个数字证书和相对应的所述复数个密钥来对所述复数个已认证身份信息和所述复数个已认证 ([1] 11/11/2025 11:11:11)

[权利要求 2]

如权利要求1所述的基于IPv6的多要素认证根系统，还包括：

绑定模块，耦接于所述第一摄取模块和所述第二摄取模块，用于将所述企业码与所述IPv6数字地址进行绑定，并生成基于IPv6的域名。

[权利要求 3]

如权利要求1所述的基于IPv6的多要素认证根系统，还包括：

笔画数字化模块，耦接于所述第一撷取模块，用于根据笔画数字代码表将所述复数个身份信息中的每一个中文文字转换成一组数字代码。

[权利要求 4]

如权利要求1所述的基于IPv6的多要素认证根系统，还包括多模块，耦接于所述根证书签发模块，所述多模块包括：中央控制模块，以及与所述中央控制模块相连接的通信模块、身份认证模块、密钥模块以及存储模块；

所述通信模块，用于实现所述基于IPv6的多要素认证根系统与外部服务器的通信；

所述身份认证模块，用于对所述用户输入的生物识别数据进行认证以生成已认证生物识别数据，并于认证通过后，对所述用户进行授权；

所述密钥模块，用于存储所述复数个密钥，并根据所述复数个密钥中相对应的密钥来对所述复数个已认证身份信息和所述复数个已认证企业信息进行加密，以生成复数个加密的已认证身份信息和复数个加密的已认证企业信息；

所述存储模块，用于存储所述已认证生物识别数据、所述复数个加密的已认证身份信息、所述复数个加密的已认证企业信息、所述电子名章、所述电子公章和所述复数个根证书；并且

所述中央控制模块，用于接收输入并控制其他模块的操作，并在所述用户获得授权后，允许所述用户调用所述电子名章和所述电子公章。

[权利要求 5]

如权利要求1所述的基于IPv6的多要素认证根系统，其特征在于：所述企业码是以固定电话号码进行绑定，且所述固定电话号码是符合全球性金融安全级别的数字化应用。

[权利要求 6]

如权利要求1所述的基于IPv6的多要素认证根系统，其特征在于：所述基于IPv6的多要素认证根系统是全球全局性数字化应用的证密链操作系统。

- [权利要求 7] 如权利要求1所述的基于IPv6的多要素认证根系统，其特征在于：
所述电子名章在盖章时还需要手写签名。
- [权利要求 8] 一种基于IPv6的多要素根认证方法，应用于基于IPv6的多要素认证根系统，包括以下步骤：
提供所述基于IPv6的多要素认证根系统，所述基于IPv6的多要素认证根系统包括第一撮取模块、第二撮取模块、第三撮取模块、信息认证模块、电子名章/公章生成模块以及根证书签发模块；
利用所述第一撮取模块，来取得用户的复数个身份信息、复数个企业信息和企业码；
利用所述第二撮取模块，来取得所述用户的IPv6数字地址，其中所述IPv6数字地址包括复数组十六位地址片段；
利用所述第三撮取模块，来取得复数个数字认证中心所提供的复数个数字证书和相对应的复数个密钥；
利用所述信息认证模块，来根据所述IPv6数字地址的所述复数组十六位地址片段对所述用户的所述复数个身份信息和所述复数个企业信息进行实体或数字化认证，并生成复数个已认证身份信息和复数个已认证企业信息；
利用所述电子名章/公章生成模块，来根据所述用户的所述复数个已认证身份信息和所述复数个已认证企业信息来生成所述用户的电子名章和电子公章；
利用所述根证书签发模块，来在所述用户发出根证书签发请求时，通过所述第三撮取模块链接所述复数个数字认证中心，根据所述复数个数字证书和相对应的所述复数个密钥来对所述复数个已认证身份信息和所述复数个已认证企业信息进行多密钥验证，并签发复数个根证书。
- [权利要求 9] 如权利要求8所述的基于IPv6的多要素根认证方法，还包括以下步骤：
基于IPv6的多要素认证根系统还包括绑定模块；

利用所述绑定模块，来将所述企业码与所述IPv6数字地址进行绑定，并生成基于IPv6的域名。

[权利要求 10] 如权利要求8所述的基于IPv6的多要素根认证方法，还包括以下步骤：

基于IPv6的多要素认证根系统还包括笔画数字化模块；

利用所述笔画数字化模块，来根据笔画数字代码表将所述复数个身份信息中的每一个中文文字转换成一组数字代码。

[权利要求 11] 如权利要求8所述的基于IPv6的多要素根认证方法，还包括以下步骤：

提供中央控制模块，以及与所述中央控制模块相连接的通信模块、身份认证模块、密钥模块以及存储模块；

利用所述通信模块，来实现所述基于IPv6的多要素认证根系统与外部服务器的通信；

利用所述身份认证模块，来对所述用户输入的生物识别数据进行认证以生成已认证生物识别数据，并于认证通过后，对所述用户进行授权；

利用所述密钥模块，来存储所述复数个密钥，并根据所述复数个密钥中相对应的密钥来对所述复数个已认证身份信息和所述复数个已认证企业信息进行加密，以生成复数个加密的已认证身份信息和复数个加密的已认证企业信息；

利用所述存储模块，来存储所述已认证生物识别数据、所述复数个加密的已认证身份信息、所述复数个加密的已认证企业信息、所述电子名章、所述电子公章和所述复数个根证书；

利用所述中央控制模块，来接收输入并控制其他模块的操作，并在所述用户获得授权后，允许所述用户调用所述电子名章和所述电子公章。