基于 PKI 与 PMI 的海洋政务服务系统安全解决方案的设计与实现

任兴元[1] 王佳慧[2] 马利民[3] 郭晓蕾[4]

[1](国家海洋信息中心 天津 300171)

[2](国家信息中心 北京 100045)

[3](北京信息科技大学 北京 100101)

[4](北京宇航系统工程研究所 北京 100076)

摘 要 海洋政务部门建立的信息管理系统有效地提高了业务效率和服务水平,但是该系统尚未建立有效的安全管理体系,内部信任体系建立不够完善,政务事项公文处理的有效性、及时性、机密性和完整性无法得到有效保证。针对此问题,基于 PKI、PMI 和可信时间戳等技术,提出一种综合的信息安全保障系统,满足了海洋政务系统的在身份认证、授权管理和访问控制等方面的要求。

关键词 海事信息化 PKI PMI 可信时间戳

中图分类号 TP3 **文献标志码** A DOI:10.3969/j.issn.1000-386x.2020.12.011

DESIGN AND IMPLEMENTATION OF SECURITY SOLUTION FOR MARINE GOVERNMENT SERVICE SYSTEM BASED ON PKI AND PMI

Ren Xingyuan[1] Wang Jiahui[2] Ma Limin[3] Guo Xiaolei[4]

[1](*National Marine Data and Information Service*, *Tianjin 300171*, *China*)

[2](*State Information Center*, *Beijing 100045*, *China*)

[3](*Beijing Information Science & Technology University*, *Beijing 100101*, *China*)

[4](*Beijing Institute of Aerospace Systems Engineering*, *Beijing 100076*, *China*)

Abstract The information management system established by marine government departments has effectively improved business efficiency and service level. However, the systems have not yet established an effective security management system. There are problems such as the establishment of internal trust system is not perfect, the validity, timeliness, confidentiality and integrity of document on government matters processing that cannot be effectively guaranteed. Based on PKI, PMI and trusted timestamp technology, this paper proposes a comprehensive information security system, which meets the requirements of marine information system in identity authentication, authorization management and access control.

Keywords Maritime informatization PKI PMI Trusted timestamp

0 引 言

近年来国家高度重视海事发展,在海事信息化建设方面不断加大投入,有效地提升了我国海洋信息发布与信息处理的能力和服务水平。特别在当前国家将互联网 +、大数据和人工智能提升为国家战略的情况下,需要继续提升我国海事业务的信息化建设水平、管理效能和公共服务水平[1]。目前,我国海洋政务部门针对不同的业务,已经建成了多个海洋信息管理系统。其中,洋山港海事局开发了“洋山港辖区水上交通大数据智能服务平台”,实现了多个信息系统数据的共

收稿日期:2019 - 06 - 20。中央引导地方科技发展专项(Z171100004717002);北京市教育委员会科技计划项目(KM201811232017)。
任兴元,高工,主研领域:网络安全协议,政务系统安全。**王佳慧**,博士。**马利民**,讲师。**郭晓蕾**,硕士。

享及智能分析[2]。互联网 + 海洋政务服务平台,对我国现有的海洋信息系统进行梳理,解决信息孤岛问题,实现资源整合,全面公开海洋政务服务事项,优化服务方式和服务流程,全面提升海洋部门政务服务水平。上述信息系统的建设对于我国海洋信息化推进具有重要意义,但是目前我国海洋信息系统普遍存在着重建设、轻管理的问题,特别是在信息安全管理方面,可能仅堆砌了一些防火墙、反病毒网关等安全硬件产品,而整体的安全防护规划和信息保护机制不够健全[3]。而作为信息安全最重要的服务,身份认证、访问控制机制以及电子公文的不可否认性验证技术是海洋信息系统的重要组成部分。常见的基于用户名和密码的认证方式容易遭受密码猜测攻击,而基于数字证书的 PKI (Public Key Infrastructure)公钥基础设施可以利用公钥加密技术完成对信息系统用户的身份认证[4]。用户在完成身份认证的基础上,对信息系统相关资源的访问需要进一步进行管理和授权,因为不同角色的用户具有的访问权限是不一样的,这一需求可以通过 PMI (Privilege Management Infrastructure)完成[5]。目前,研究人员已经开展了很多 PKI 和 PMI 的相关技术研究。文献[6]提出基于 PKI/PMI 的电子政务集成用户可信度的管理,以满足电子政务的安全需求。文献[7]提出 PKI 和 PMI 技术在医院信息系统中的应用,解决了电子病历系统的安全访问控制问题。文献[8]分析了在目前大数据发展趋势下,信息系统互联互通及数据共享面临的安全风险,并提出 PKI/PMI 机制解决海量数据业务应用系统面临的安全风险。政务服务事项作为海洋政务服务系统中的重要环节,其真实性、完整性和不可否认性的验证具有重要的安全意义,可信时间戳在此方面具有一定的应用价值[9-10]。文献[11]研究了税收管理系统中利用电子签章和可信时间戳技术实现电子表单的文书版式化和防篡改。文献[12]利用 PKI 技术和可信时间戳技术,实现了电子商务系统的数据完整性、电子举证和责任认定等安全功能。文献[13]研究了可信时间戳技术在医院电子档案的中实现精准可信的时间认证的应用。

本文基于 PKI、PMI 和可信时间戳等技术,结合互联网 + 海洋政务服务平台,提出一种行之有效的信息安全解决方案,主要解决目前在国家海事信息化实际建设和使用过程中面临的非法用户登录,口令猜测攻击以及政务服务过程的机密性、完整性和不可否认性的问题。同时,将该安全方案基于 C ++ 和 XML 等编程语言进行了实现,并通过实验测试验证了该安全模型在身份认证、授权管理等方面的功能。实验结果表明,该方案可以有效解决海洋政务服务系统面临的安全问题,具有较高的实用价值。

1　相关技术

1.1　公钥基础设施 PKI

PKI 以公钥加密技术为基础,基于数字证书 PKC (Public Key Certificate)来实现用户公钥与其身份的绑定,可实现数据电文的加密解密、数字签名和网络实体认证等安全服务。PKI 是一个可以支持数字证书的创建、存储和分发的框架,它能够为所有网络用户透明地提供可验证的公钥和证书管理功能。

PKI 由一个可信的认证机构(Certificate Authority, CA)通过数字签名来将用户的公钥信息和用户的其他可标识身份的信息(如姓名、身份证号等)进行绑定,确保用户身份的唯一性,用于在互联网上认证用户的身份。

PKI 通过公钥加密技术建立一整套严密的身份认证系统,它可以确保信息传输的保密性、网上通信双方身份的确定性、发送消息的不可否认性、交换数据的完整性。PKI 的基础是公钥加密技术,其中用户公钥是公开的,通过数字证书进行分发,这就使得通信双方在无须事先交换密钥信息的情况下,保证了对话的机密性、信息的完整性和用户身份的可认证。

PKI 系统是由 CA、注册机构(Register Authority, RA)、证书库(包含证书和证书撤销列表)、密钥管理中心(Key Management Center, KMC)、应用程序接口 API 等基本组成部分组成,如图 1 所示。

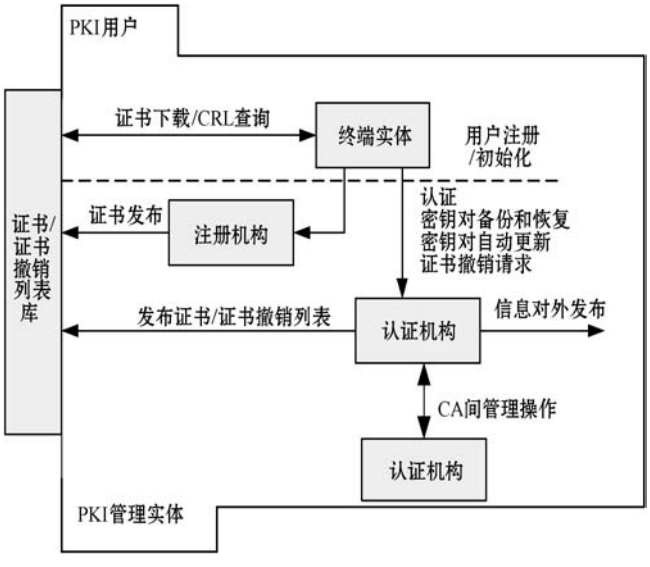

图 1　PKI 体系架构

1.2 授权管理基础设施 PMI

在 PKI 完成对用户的身份认证后,还需要完成用户个人身份认证到权限信息的映射,以实现更加安全合理的信息系统资源的访问权限控制。PMI 作为授权管理基础设施,它将访问控制模块从传统的应用系统中剥离出来,以独立的方式向用户(包括应用程序)提供授权管理和用户身份到权限信息映射的服务,提供的授权和访问控制机制的特点在于:能够根据实际应用的处理模式进行映射,而且与具体应用系统的开发及其管理没有相关性。PMI 具有以下优点:(1) 在用户的具体应用中,实现访问控制与权限管理系统的开发、维护简单化;(2) 管理成本降低;(3) 复杂性降低。PMI 建立在身份认证即 PKI 的基础上,用属性证书(Attribute Certificate,AC)容纳和标识权限信息,提供严格、灵活、高效的权限管理服务。权限的申请是通过管理属性证书的申请来实现的,类似权限的发放、使用和撤销管理也分别对应着管理属性证书的签发、验证、注销,权限与属性证书两者各自的生命周期都是有其对应关系的。

PMI 的体系结构主要包括以下几个部分:信任源点(Source of Authority,SOA),属性权威(Attribute Authority,AA)、特权验证者(Privilege Verifier,PV)、AA 代理(AA Agent)、证书库和通信协议,如图 2 所示。

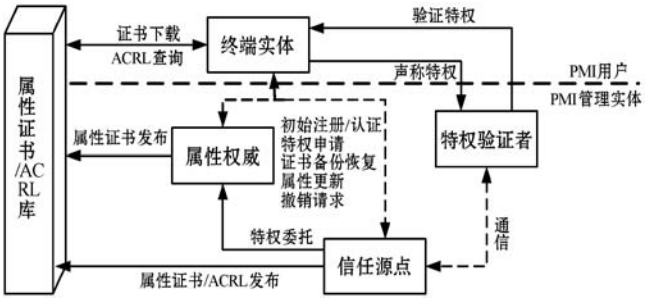

图 2 PMI 体系架构

1.3 基于角色的访问控制 RBAC

RBAC 模型基于角色的访问控制模型,现在常用于实现信息系统的权限管理设计。其基本思想是在实际应用系统中根据不同的职能岗位划分出对应角色,角色与访问权限相关,并且分配给用户,角色集由会话激活,使用户能够间接地通过角色访问目标资源。用户与角色、操作权限与角色都是多对多的关系,即多个角色可以分配给一个用户,多个用户可以使用一个角色[15]。基于角色的访问控制可以更好地模拟实际生活中的职责关系,又可以制定和管理授权策略,灵活度较高。在 PMI 中使用基于角色的访问控制,为用户签发角色分配证书,用户角色权限变更时,不必撤销颁发给用户的属性证书,只需要变更角色规范证书中对应的权限,极大减少了系统开销,具有强大的可操作性。

1.4 可信时间戳

数字签名和时间戳服务是电子文件签名领域的两种签名形式,两种签名是互不冲突的。数字签名解决了签名人身份的真实性和数据电文内容的完整性,但其存在着有效期,用户密钥可能丢失和用户可随时吊销证书的问题,导致证书持有者有否认签名的可能,无法确认签名的有效性,且对于时间不能保证。可信时间戳技术可以解决上述问题,同时对数据电文进行数字签名和添加第三方可信时间戳,在需要时既可以保障数据电文的完整性、真实性,又可以确认签名时的数字证书是否在有效期范围之内,且与数字签名搭配后才能彻底解决电子公文的法律效力和责任认定的问题。

可信时间戳是由一个被法律和公众认可的第三方充当时间戳服务中心(Time Stamp Authority,TSA),用其私钥对数据和相关信息签名形成的具有法律效力的数字凭证,其中包含对数据摘要形成的“指纹”、TSA 收到请求的时间、时间戳服务中心的相关信息等。它能证明一个文档在某个时间点是否已存在以及完整性,且与电子数据唯一对应。时间戳组成如图 3 所示。

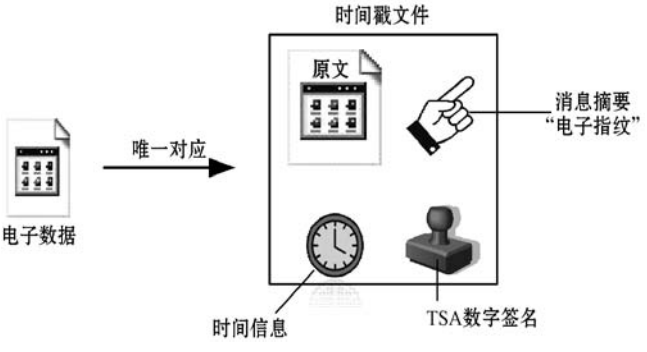

图 3 时间戳组成

2 平台设计

本文在对身份认证技术、授权管理技术、访问控制技术和可信时间戳技术研究的基础上,建立了一个安全可信的互联网 + 海洋政务服务平台。系统实现了对用户统一身份认证,对于不同用户,根据给不同的身份授予不同的访问操作权限,使他们能够进行相应授权的访问和操作,从而保障了互联网 + 海洋政务服务平台信息资源的安全访问。同时,系统还融合了可信时间戳技术为整个系统提供时间保障和确认机制。本系统结构如图 4 所示。

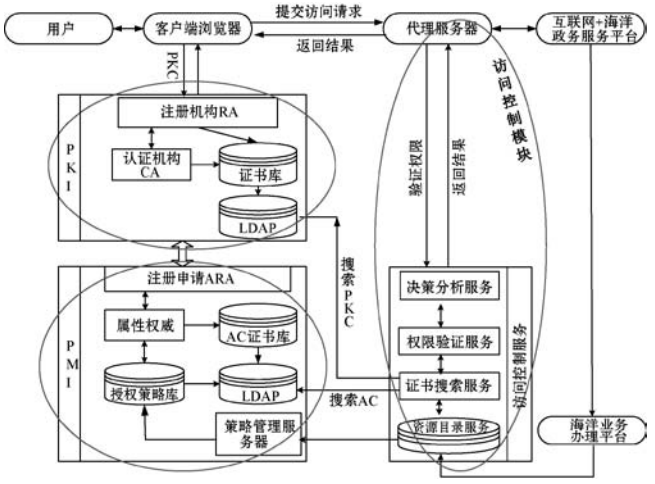

图 4　安全的互联网 + 海洋政务服务平台

1）互联网 + 海洋政务服务平台建立了一套完整的 PKI 认证系统,为各个本系统的用户统一签发数字证书 PKC,提供用户在互联网的安全认证服务。系统集成公钥证书的应用,在用户登录系统时,必须提交权威认证机构 CA 颁发的用户证书,通过证书来实现身份认证,同时通过公钥加密技术和数字签名技术,实现相关电子公文传输的机密性和抗抵赖性等安全需求。

2）实现对不同用户统一的权限管理。完善权限认证,系统赋予互联网 + 海洋政务服务平台中不同职责用户不同的角色,不同角色对应不同的权限,不同的权限对应着海洋政务服务平台不同的访问和操作功能,实现安全访问控制,防止非法访问和篡改电子公文信息。

3）可信时间戳是时间戳服务中心 TSA 用自己的私钥对数据和产生时间进行签名得到的,TSA 必须由可信任的第三方机构担当,而时间必须由权威授时中心来负责保障其准确可靠性,任何个人和机构不能对时间进行修改以保障某一文件或操作在某一时间已存在时间的权威,为互联网 + 海洋政务服务平台提供具有法律效力的时间证据。

2.1　身份认证模块

身份认证模块为整个互联网 + 海洋政务服务平台的用户颁发数字证书用于身份认证,当然包括应用程序、服务中心,以及可信时间戳服务中心 TSA 的数字证书,但其证书扩展中的增强型用法要明确标识为时间戳。以政务服务服务管理系统为例,在用户访问政务服务服务管理时进行身份验证,确保其公钥证书的有效性。

用户首先要申请自己的公钥证书,如图 5 所示,用户需要填写自己的个人信息,然后客户端生成一对密钥,私钥由用户自己保存,且需要口令保护,公钥和个人信息一起生成请求信息提交给注册机构 RA,等待审核。

图 5　PKI 证书申请页面

RA 管理员登录到 PKI 系统,查看用户的证书请求,审核用户的信息,对证书请求进行验证,如同意为用户颁发证书,则对用户申请信息签名后发送给 CA,由 CA 为用户签发证书,如图 6 所示。

图 6　管理员处理证书请求页面

用户获得证书后,就可以在网络上进行身份认证,提交公钥证书后,证书验证通过后可登录互联网 + 海洋政务服务平台。基于公钥数字证书实现身份认证可以有效解决传统认证方式面临的口令猜测攻击问题,有效提高信息系统安全性。图 7 为互联网 + 海洋政务服务平台登录界面。

图 7　互联网 + 海洋政务服务平台登录界面

2.2　授权管理与访问控制

2.2.1　授权管理模块

互联网 + 海洋政务服务平台的用户主要分为四大

类型:自然人/法人,事项受理人员,业务办理人员,系统管理人员。实际应用中,可根据工作职责进行更细粒度的角色划分和定义。根据 RBAC 最小权限原则,所有用户都可申请公钥证书和属性证书,验证公钥证书和属性证书,以及凭公钥证书登录查看自己的基本信息。

由此,本文根据四大类型人群所访问和操作政务事项的性质做出如下四类角色的定义和权限划分:

1) 公众通过互联网访海洋政务服务门户网站,申请相关的政务服务。系统则需要为每一个公众用户分配唯一的公钥证书,以确保用户认证的安全性。在系统中,具体事务办理的内容可根据安全保密程度设立在安全标签属性中设立安全级别,同时在属性证书中分配相应的安全级别。然后为公众用户设定合理的访问权限,根据安全级别从低到高来访问,其具有的权限如图 8 所示。

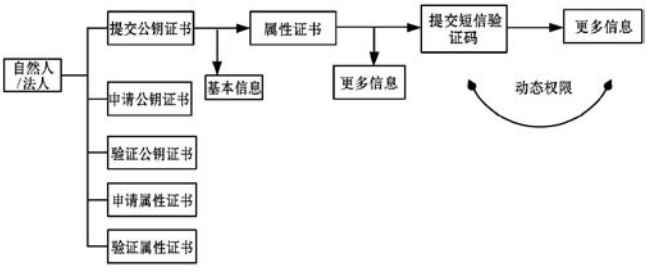

图 8 海洋政务系统用户权限管理

通过提交自己的公钥证书后,可以看到自己政务事项办理的基本信息;如:姓名、年龄、电子邮箱、联系方式、事件办理进度等内容。此外,用户通过公钥证书 + 角色为自然人/法人的属性证书 + 验证码 + 短信(动态令牌),可动态提升访问权限级别,查阅更多信息。

2) 海洋政务事项处理人员通常具有两种角色,政务大厅受理人员和海洋政务事项办理人员,其访问权限如图 9 所示。

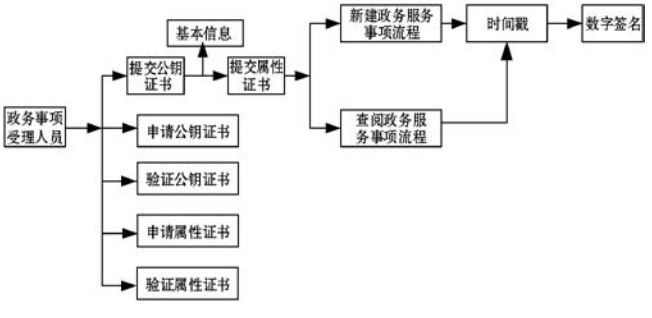

图 9 海洋政务系统事项受理人员权限管理

(1) 作为政务大厅受理人员,可以通过互联网 + 海洋政务服务平台,采用公钥证书 + 作为受理人员角色的属性证书的认证方式登录,可查阅、新建事项办理信息。

同时,出于对政务事项的安全性的保护以及明确政府办公人员责任,政务大厅受理人员在以事项受理人员角色登录后,如果要查阅或新建政务事项办理信息,需要在修改后的文件后加盖可信第三方的时间戳,然后用自己的私钥进行数字签名。政务事项办理人员权限管理如图 10 所示。

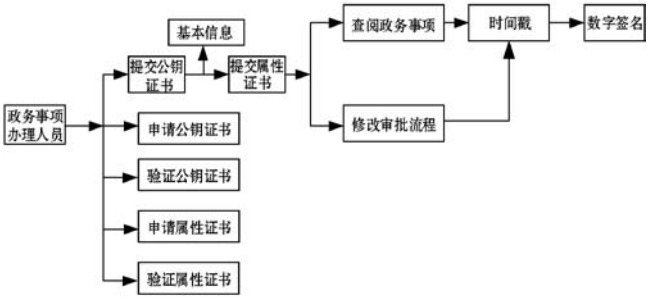

图 10 海洋政务系统事项办理人员权限管理

(2) 作为业务办理人员,主要负责对已受理的政务事项按照相关部门规定,进行审核和办理,需要验证已提交的事项办理相关材料的真实有效性以及是否齐全。若齐全则审批通过,事项办理进入下一个流程环节;否则退回处理,此时事项申请的自然人/法人可以在自己的系统页面内看到事项办理的进度以及是否成功或失败的原因。业务办理人员在完成政务事项审批之后,要添加时间戳并用自己的私钥进行数字签名备档。最后添加归档时间,添此后,政务事项审批流程便不可再被更改。

3) 授权管理人员主要负责对系统内用户进行授权,在用户提交证书申请信息后,查看用户的请求,进行核实之后,为用户签发证书。在本系统中管理员角色一分为二,分别负责 PKC 和 AC 的请求管理和核实签发。本文中为了简便明了,仅定义为一个角色,其权限信息如图 11 所示。

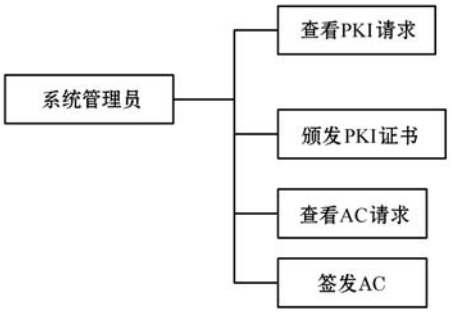

图 11 系统管理员权限

所有用户需要行使以上角色的权限都要先申请该角色的属性证书。用户在申请属性证书 AC 时首先要对用户进行身份认证,具体过程如下:① 用户在客户端向属性权威提交代表身份的公钥证书,属性权威发送给申请者一个随机数 X,申请者用他的私钥 RK 对 X 进行签名,即 $Sig(X,RK)$,属性权威根据申请者的公钥

PK 验证其签名的真实性,如果签名确实由用户的私钥产生,则认为该申请者确实为公钥证书持有者本人,即通过身份认证。② 属性权威验证通过之后,用户继续提交申请所需的角色及申请该角色需要提交的个人信息,请求属性权威签发相应的属性证书。属性权威将请求信息进行保存,由系统管理人员核查用户提交的信息以及用户和所申请角色是否相符之后进行决策判断,审核通过后属性权威用自己的私钥为 AC 申请者签发属性证书。系统将证书可放在用于提供目录服务的数据库供用户查询下载属性证书。具体申请流程如图 12 所示。

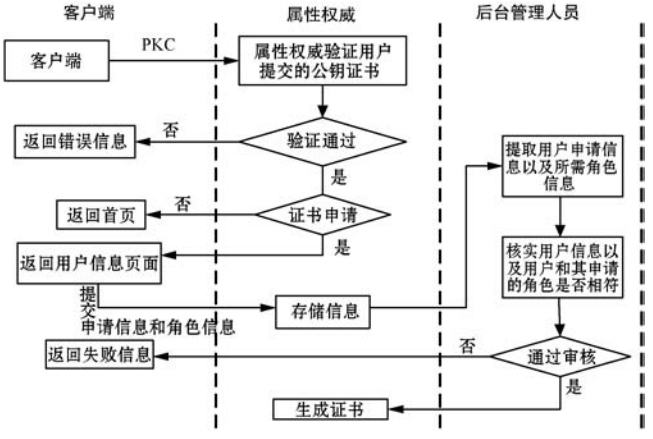

图 12　用户属性证书申请流程

授权管理模块还要提供可验证属性证书的服务供访问控制模块调用,包括:验证用户的属性证书的签名的正确性,确保其由属性权威的公钥签名形成;验证用户属性证书的有效性,确保属性证书仍在有效期范围内;验证属性证书的签发者的权威性,确保其为可信任的授权者。

2.2.2　访问控制模块

因为整个系统建立在身份认证的基础上,所以需要用户用自己的公钥证书登录系统,提交证书后,访问控制模块调用 PKI 系统身份认证服务接口的证书验证服务,核实用户的身份,在验证之后由访问控制模块将决策结果返回用户的基本信息页面,包括姓名、年龄等。

在用户想要更多权限时,可以提交自己的属性证书。访问控制模块必须确保用户的角色分配属性证书与用户提交的公钥证书的关联性,属性证书的持有者应与公钥证书的持有者相同或公钥证书的颁发者标识和序列号与属性证书 ID 号相关联,以防非冒名使用用户的权限。调用授权管理模块提供的验证服务接口验证用户提交的属性证书,确保其有效性。然后从属性证书提取用户的角色信息,根据其角色信息和授权策略,判断用户角色的权限是否包含执行该请求的最小权限集,决定用户是否可以执行该请求,如果用户角色权限覆盖请求操作,则返回给用户请求的目标资源页面,否则返回用户信息页面,对海洋政务系统平台进行严格的访问控制。流程如图 13 所示。

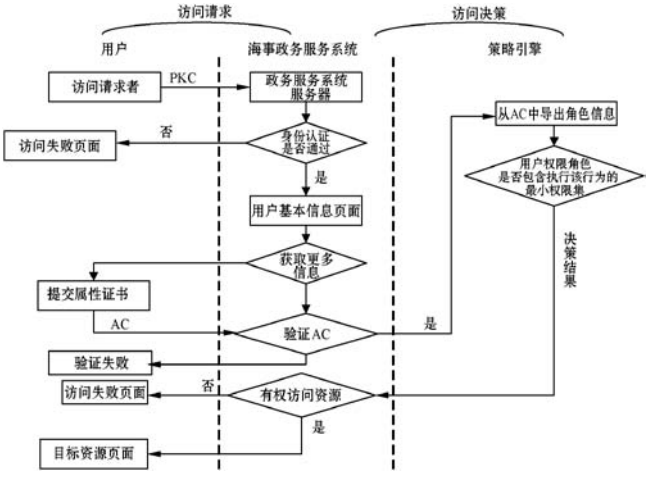

图 13　用户访问权限控制过程

2.3　可信时间戳模块设计

可信时间戳为海洋政务服务管理平台提供准确可靠的时间。政务办理人员在对政务事项进行操作之后,若需修改,要进行数字签名来确认,以供必要时查证。然而政务办理人员用于签名的公钥存在有效期和丢失问题,存在不承认签名的可能。故本文添加了时间戳系统为数字签名提供准确可靠的时间。可信时间戳服务中心应由国家权威授时中心进行守时和授时,本文中用系统时间代替,可信时间戳模块的设计如图 14 所示。

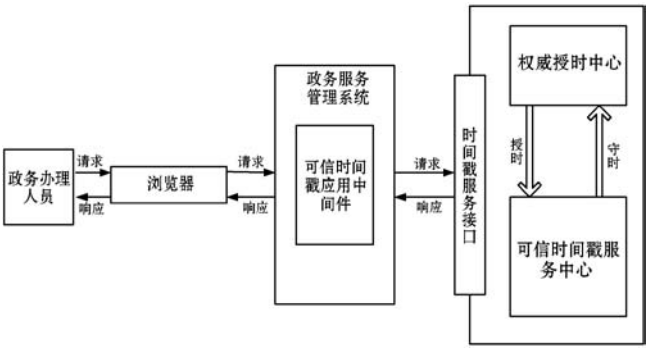

图 14　可信时间戳模块架构

可信时间戳的申请流程如下:

1)政务办理人员使用数字证书登录海事电子安全系统后,指定政务事项处理公文,客户端程序对政务事项处理公文提取指纹(Hash 值),这样可信时间戳中心也不能看到政务事项处理的内容,保证机密性和隐私性。

2)提交政务事项处理公文的摘要信息到可信时间戳系统,请求加盖时间戳。

3)可信时间戳服务中心收到请求信息后,添加收

到请求时的时间,用自己的私钥进行签名后形成时间戳返回给用户。

4)保存政务事项处理公文指纹和时间戳到数据库。

5)政务办理人员收到时间戳后,将时间戳和政务处理事项一起进行数字签名,然后存储到数据库,若添加时间戳后不进行签名,则之前的操作将不被保存。

图 15 为本文中申请时间戳和响应的页面。可看到,首先选择形成时间戳请求的参数信息,哈希算法是指对文件进行摘要的算法,系统提供了 SHA1 和 MD5 两种;策略是指时间戳服务中心签发时间戳的策略,本文中为可签发所有数据电文的策略;no_nonce 指是否在请求中添加一个很大的随机数,若添加,时间戳响应中也必须有此值,且不能改变,否则用户有理由相信时间戳出错;cert 是指是否在时间戳响应中携带时间戳服务中心的数字证书。选择参数完毕后可点击发送,由时间戳服务中心返回时间戳。

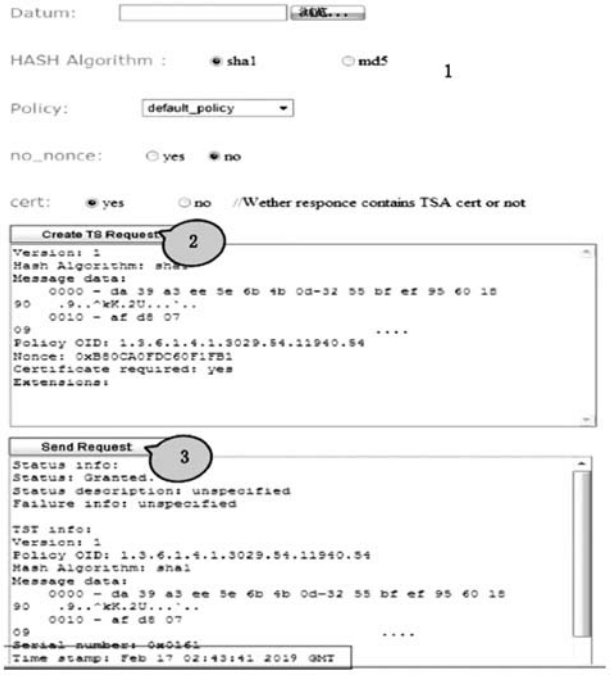

图 15 可信时间戳申请及相应详情

可信时间戳的验证流程为:(1)用户使用数字证书登录海事政务服务管理系统后,指定政务服务事项,用浏览器程序对其提取电子指纹,将时间戳和指纹一起发送给时间戳服务中心请求验证。(2)时间戳服务中心 TSA 收到请求后,用自己的私钥对时间戳进行解密提取摘要信息,然后和用户发送的摘要信息进行对比,若一样则认为该文件是在时间戳中包含的时间已存在,反之则认为文件已被修改。若用户只发送了摘要信息,则 TSA 还需到数据库根据摘要信息查找时间戳。(3)返回政务服务事项处理的有效性检查结果(是否被篡改、加盖时间戳时间信息)。

3 安全性和效率分析

本文的互联网 + 海洋政务服务平台的安全解决方案可以有效解决互联网 + 海洋政务服务平台面临的一系列安全问题,如:口令猜测攻击,政务事项处理的机密性、数据完整性鉴别问题和责任认定问题。

口令猜测攻击:基于公钥加密技术和数字证书的 PKI 框架在实现用户身份认证时,完全基于 CA 对用户数字证书有效性的验证,因此不存在口令猜测攻击问题。由于本系统基于公钥加密技术,证书验证时间比基于用户名/口令验证时间要长,但是安全性有了很大程度提高。

政务事项处理过程的机密性、完整性鉴别问题:本文基于公钥加密技术,将系统内发出的政务事项处理公文在传输过程中实现加密,同时基于业务办理人员的私钥进行签名。签名完成后,需要向可信时间戳服务中心申请加盖时间戳,确保政务事项处理公文在流转过程中的机密性、完整性及不可否认性。

责任认定:政务事项处理公文在传输及阅读过程中,根据不同角色具有的相应权限,可以由某些人员对政务事项处理公文进行修改,然而每次修改完成后,按照系统要求,需要用自己的私钥进行签名并且加盖时间戳,进一步提升政务事项处理流程的法律举证作用。

4 结 语

本文基于 PKI、PMI、RBAC 和可信时间戳技术,结合互联网 + 海洋政务服务平台,设计并实现一种用于互联网 + 海洋政务服务平台的安全解决方案,为保障海洋政务信息化奠定了安全基础。系统运行结果表明,所开发的系统是一个安全可信的、统一的、完整的安全认证及权限统一管理与服务的平台,可以有效保障海洋政务系统中用户的身份认证及政务事项处理的完整性、机密性、不可抵赖性以及法律效力。下一步工作将针对海洋政务服务平台提供安全的数据共享服务展开研究,在进一步加强海洋政务数据安全性的同时,实现海洋政务数据的分级分类整理,为其他信息系统提供数据共享服务,打破信息系统之间的隔阂,早日实现海洋政务数据共享和大数据分析,简化办事流程,提高服务效率。

参 考 文 献

[1] 陈勇剑,周敬祥,王超亮. 基于“互联网 + ”技术的海事信

息化“十三五”建设规划[J]. 水运工程,2016(10):174 - 176,194.
[2] 刘伟荣,徐凯,董大伟. 海事信息化发展新趋势[J]. 中国船检,2017(10):76 - 78.
[3] 王军. 海事信息安全关键技术研究[J]. 交通信息与安全,2010,28(6):88 - 90.
[4] 张瑞,舒虹. 基于 PKI 的网络云认证系统设计[J]. 现代电子技术,2017,40(23):81 - 84.
[5] 罗霄峰,王文贤,罗万伯. 访问控制技术现状及展望[J]. 信息网络安全,2016,16(12):19 - 27.
[6] 宋福英. 电子政务集成用户可信度的 PKI/PMI 安全机制的研究[J]. 智能计算机与应用,2016,6(3):81 - 83.
[7] 刘光磊,肖辉. PKI 与 PMI 技术在医院信息系统中的应用[J]. 中国数字医学,2018,13(3):99 - 101.
[8] 刘西薇. 数据大集中下的授权方案[J]. 信息安全与通信保密,2014(9):160 - 162.
[9] Internet X.509 public key infrastructure time-stamp protocol (TSP):RFC3161[S/OL]. USA:IETF,2001. [2019 - 06 - 20]. https://www. rfc-editor. org/rfc/inline-errata/rfc3161. html.
[10] 蹇文燕. 在电子档案管理中引入可信时间戳[J]. 山西档案,2016(2):37 - 39.
[11] 宋峻超,王跃,宋兴彬. 电子签章和版式文件在无纸化办税中的应用研究[J]. 计算机应用与软件,2019,36(2):131 - 134.
[12] 祁凯. 可信数据保全系统的设计与实现[J]. 网络空间安全,2018,9(12):7 - 13.
[13] 王文翠,李志强,秦芳等. 基于数字签名的可信电子病历系统[J]. 中国数字医学,2016,11(3):19 - 21.
[14] Mitra B, Sural S, Vaidya J, et al. Migrating from RBAC to temporal RBAC[J]. IET Information Security,2017,11(5):294 - 300.
[15] 顾春华,高远,田秀霞. 安全性优化的 RBAC 访问控制模型[J]. 信息网络安全,2017,17(5):74 - 79.

(上接第 16 页)

时间会产生比较大的性能滑坡。采用多环形队列共享内存异步传输数据同步对共享空间访问进行优化,可以显著提升系统性能,其传输延迟和吞吐量受客户端数量影响不大。

5　结　语

测试指挥显示系统将试验中的态势数据、关键设备测试数据、实时监视视频、指令进程数据、调度语音、气象数据、电磁环境参数、靶标毁伤数据,以及各类数据统计结果进行综合显示,是试验指挥决策的关键环节。系统进程间数据的同步效率,直接影响其效能的发挥。本文针对较大数据量的数据同步问题,设计一种基于多环形队列共享内存异步传输数据同步方法,替代传统的内存数组的共享方式,很好地解决了大数据量汇集时共享内存数据同步效率降低的问题,提高了系统的适应性和可靠性,也为设计需要汇集较大数据量,且有多个进程进行数据同步协同工作类似指挥显示系统软件提供很好的解决思路。

参　考　文　献

[1] 王皓,王欣然,过其峰,等. 一种基于共享内存的消息总线设计与实现[J]. 电子科技,2017,30(9):93 - 96,104.
[2] 胡亮,王敏珍,蒋春晓,等. 机内进程间通信的性能测试和评价[J]. 吉林大学学报(信息科学版),2003,21(4):417 - 420.
[3] 苏红旗,刘官树. 一种基于内存共享的高效进程间通信机制[J]. 新型工业化,2014,4(2):67 - 73.
[4] 王瑾,彭晖,侯勇. 基于共享内存的能量管理系统实时库非主键 HASH 索引[J]. 电力系统自动化,2011,35(13):72 - 76.
[5] 连仁包,王卫星. 基于共享内存的松耦合日志系统研究和设计[J]. 计算机应用与软件,2013,30(6):8 - 11,15.
[6] 刘虎球,赵鹏. 一种多核间内存公平调度模型[J]. 计算机学报,2013,36(11):2191 - 2199.
[7] 苗乾坤. 面向共享存储系统的计算模型及性能优化[D]. 合肥:中国科学技术大学,2012.
[8] 余翔湛,殷丽华. 动态共享内存缓冲池技术[J]. 哈尔滨工业大学学报,2014,36(3):380 - 383.
[9] 郑艳. 利用共享内存实现进程间高效率数据共享[J]. 城市建设理论研究,2012(2):1 - 3.
[10] 张居瀚. 基于 NoC 架构的分布式共享内存管理系统的实现和验证[D]. 上海:复旦大学,2014.
[11] 罗毅. 基于 PCM 的混合内存系统的研究与仿真[D]. 武汉:华中科技大学,2014.
[12] 周恒钊. 面向大规模分布式共享内存系统的 Cache 一致性协议研究和实现[D]. 北京:中国科学院大学,2016.
[13] 孟晓林. 多核系统减少内存干扰技术的研究[D]. 杭州:杭州电子科技大学,2016.
[14] 彭煜. 机动车事故责任纠纷智能辅助审理系统的设计与实现[D]. 南京:南京大学,2018.
[15] 张波. 军用电源模块自动化测试系统的设计与实现[D]. 北京:中国科学院大学,2014.
[16] 宋晗. 卫星测试数据管理系统的设计与实现[D]. 西安:西安电子科技大学,2017.
[17] 丛一. 基于 GIS 的警用应急指挥及预案管理信息系统的设计与实现[D]. 内蒙古:内蒙古农业大学,2017.