●李 纲 王毅彦

电子政务信息安全平台分析*

摘 要 信息安全平台是保护网上政务资源的整体性解决方案。整个信息安全平台由安全支撑平台和安全应用支撑平台构成。安全支撑平台基于公钥基础设施和授权管理基础设施构建。安全应用支撑平台直接为本地的业务系统提供多种安全服务。图4。参考文献7。

关键词 电子政务 信息安全 信息安全平台

分类号 G250.76

ABSTRACT Information security platform is an integrated solution to protect the resources of e-government It consists of information security support platform and security application support platform. In this paper, the authors analyze some details of the platform. 4 figs. 7 refs.

KEY WORDS e-Government. Information security. Information security platform.

CLASS NUMBER G250.76

传统的网络和系统安全大多是通过防火墙、入侵检测、漏洞扫描、网络隔离等技术和设备来实现,在一定程度上可以保证信息系统的安全,但是不能有效满足国家电子政务对信息安全的要求。这是由于电子政务建设大量采用了国外的技术和产品,处理、传输和交换平台存在着相当大的安全漏洞和隐患。另外,电子政务对安全的需求是全面的,如信任与授权服务是传统方式难以胜任的。于是,建立完整的电子政务信息安全平台的解决方案就应运而生。

1 系统架构及组成

信息安全平台是保护网上政务资源的整体性解决方案。整个信息安全平台由两部分构成:安全支撑平台和安全应用支撑平台(如图1)。

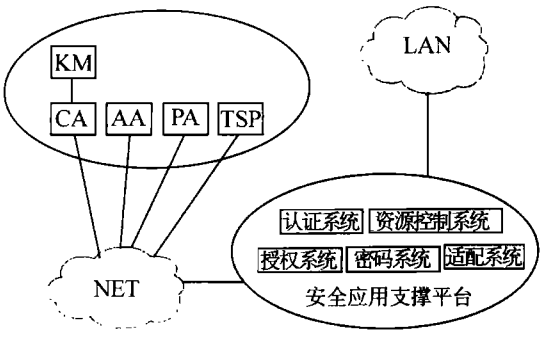

图1 国家电子政务信息安全平台示意

图1中LAN是指各行政机关内部的办公局域网,分别运行决策指挥、宏观调控、行政执行、应急指挥、监督检查、信息查询等电子政务应用系统。很多电子化的政务数据和信息资源也都放在局域网上。NET通常是指政务专网,它建立在公共通信基础设施之上,连接各个部门、各个地方的办公局域网,形成全国性的政务资源网络并承载政府系统共建共享的政务资源信息库。

图1中左上与NET连接的部分构成安全支撑平台,主要部件包括认证中心(CA)、授权中心(AA)、策略中心(PA)、时间戳服务(TSP)和密钥管理(KM)。安全支撑平台建在NET上,为整个政务系统建立起一个基本的安全支撑环境,通过CA和AA给用户发放数字的"身份证"和"工作证";通过TSP和KM为用户提供时间戳服务和密钥管理服务;通过PA进行安全策略的管理,实现政务网络各平台之间的安全的互通互信。

图1中右下分别与NET和LAN相连的部分是安全应用支撑平台。主要部件包括:认证系统、资源控制系统、授权系统、密码系统和适配系统。该平台建在本地,为本地网络中的政务应用和政务资源提供保护。NET上的用户访问LAN网要持有效的数字证书并经认证系统认证通过后方可进入;而用户要访问LAN网上的资源,则需要根据其属性证书由授权系统进行授权。如果说认证系统是本地网络的人口守护者,那么资源控制系统就是本地网络的出口守护者,它可以控制本地资源的流出。密码系统提供保密和信任服务,如加密、解密、签名和验签。适配系统通过把安全支撑平台上与本地有关的各种证书同步到本地,来提高本地安全应用支撑平台的运行效率。

国家电子政务信息安全平台在逻辑上分为两层(见图2):安全支撑平台位于底层,为政务网络构建统一的信任服务体系,是安全应用支撑平台运作的基础;安全应用支撑平台介于安全支撑平台与政务应用系统之间,直接为政务应用

* 本文系国家社会科学基金项目(04BTQ016)研究成果。

系统提供安全和信任服务。

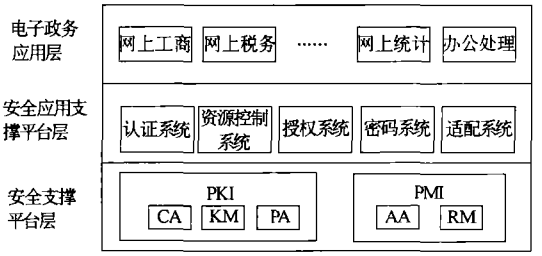

图 2　国家电子政务信息安全平台分层逻辑模型

2　基于 PKI,PMI 的安全支撑平台

安全支撑平台是构筑电子政务决策支持及公众服务系统的安全基础,它基于公钥基础设施(PKI:Public Key Infrastructure)和授权管理基础设施(PMI:Privilege Management Infrastructure)构建。PKI 为国家电子政务系统提供信任服务体系和全面的信任服务;PMI 以 PKI 的身份鉴别体系为基础,向国家电子政务系统提供有效的授权服务体系,向政务应用系统提供全面统一的授权管理和访问控制服务。

2.1　公钥基础设施

PKI 技术是建立信任服务体系的关键,也是整个政务信息安全平台的基础。信任服务体系主要是为网络信息空间提供一个信任的基准,即在用户实体和虚拟网络空间中的用户角色之间建立起映射关系,以便能将现实物理世界中的信任关系移植到虚拟的网络空间。公钥基础设施通过公钥数字证书的方式为每个合法用户提供合法的身份证明,并通过公钥密码体制中用户私钥的机密性来提供用户身份的惟一性验证,在用户的实体身份与数字证书的 ID 号间建立起惟一的映射关系。

在电子政务中,社会信任服务管理体系不仅仅要管理作为"自然人"的用户,还要管理机构和信息设备。安全支撑平台利用 PKI 技术,通过分别发放自然人数字证书、机构数字证书和信息设备数字证书,实现对这三类实体的管理,为国家电子政务建立全面、完善的信任管理体系。

2.2　授权管理基础设施

授权管理基础设施可将访问控制机制从具体应用系统的开发和管理中分离出来,使访问控制机制与应用系统之间能灵活而方便地结合和使用。

授权管理基础设施向用户发放属性证书,提供授权管理服务;它以资源(包括信息资源和应用资源)管理为核心,将对资源的访问控制权统一交由授权机构进行管理,提供与实际处理模式相应的、与具体应用系统开发和管理无关的授权和访问控制机制。它需要公钥基础设施提供身份认证服务。同公钥基础设施相比,两者的主要区别在于:PKI 证明用户是谁,并且由各类应用共同信任的有关机构提供统一管理;而 PMI 证明这个用户有什么权限,能干什么,为各类应用提供相对独立的授权管理,并且各类应用相互之间的权限资源独立。

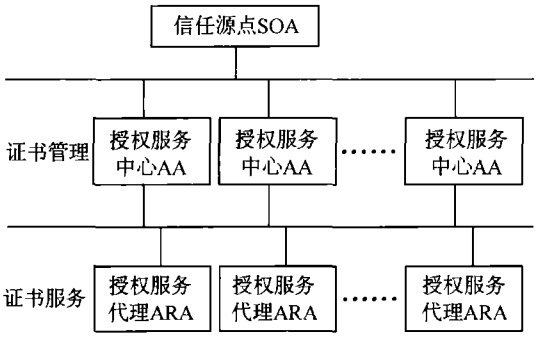

图 3　PMI 体系结构

授权管理基础设施在体系上可以分为三级(见图 3),分别是信任源点(SOA),属性权威机构(AA)和授权服务代理(ARA)。信任源点是整个授权管理体系的中心业务节点,也是整个授权管理基础设施的最终信任源和最高管理机构。SOA 的职责主要包括:授权管理策略的管理、应用授权受理、AA 中心的设立审核和管理及授权体系业务的规范化等。属性权威机构 AA 是授权管理基础设施的核心服务节点,是对应于具体应用系统的授权管理分系统,由具有设立 AA 中心业务需求的各应用单位负责建设,并与 SOA 中心通过业务协议达成相互信任的关系。AA 中心的主要职责包括:应用授权受理、属性证书的签发和管理,以及 ARA 的设立审核和管理等。ARA 中心是授权管理基础设施的用户代理节点,是与具体应用用户的接口,ARA 中心的主要职责包括授权服务代理和授权审核代理等。

3　安全应用支撑平台

安全应用支撑平台为本地政务网络构筑一个安全的工作环境,本地政务网络中所有的业务系统都工作在这个环境中。安全应用支撑平台直接为本地的业务系统提供多种安全服务。实现安全应用支撑平台需要若干主要部件。

3.1　认证系统

认证系统提供本地政务网络的接入认证服务。它可以是一个单独的网络设备(如认证网关),采用断路方式联通本地网络与其他网络。其工作原理是:利用工作在 IP 层的网络互联设备,检测、侦听所有经过的 IP 数据包。用户从政务专网或互联网访问本地网络时,必须经过认证系统。这时,认证系统检查用户 IP 数据包的源地址,如果位于该地址的用户未经认证,认证系统就要他出示数字证书。具体过程是:首先,认证系统向该地址发出一个索要证书的请求,用户收到请求后把证书提交认证系统,然后,认证系统验证这个证书,只有通过认证的用户才被允许进入本地网络。

3.2　资源控制系统

互联网为信息的传递和扩散提供了非常便捷的途径,这

就意味着政务信息可以通过这一渠道很容易的传送出去。因而，对于国家政务信息的安全来说，既要能够控制内部信息向外的流动，也要能够控制敏感信息在内部的不同组成部分之间的流动。控制信息的流出有两个解决方案：一是对内容进行过滤，敏感的信息不允许出去；二是控制信息的流向，不允许流到不安全的地方。

要对内容控制，就要对数据包进行层层的协议解析，如果内容是经过加密的，还要进行解密。此外，还要有内容过滤的标准来控制什么内容可以出去、什么内容不能出去，这些问题加在一起导致内容控制的实际操作难度很大，而控制信息的流向就要容易得多。

资源控制系统在IP层控制信息从本地网络的流出。当本地网络里面的用户要将信息往外发送时，资源控制系统检查用户IP数据包的目的地址，判断目的IP是不是授权允许出去的地址，如果这个目的地址是可信的，便允许信息发到那里。

3.3 授权系统

授权系统对本地网络中的资源进行授权，并结合PMI对用户授权形成的属性证书，在实际用户与其对资源的操作权限之间建立起映射关系。这种映射关系的建立是通过基于角色的两次授权实现的（见图4）：其一，属性权威机构AA向用户发放属性证书，属性证书通过用户公钥证书的ID号将特定的用户角色绑定到对应的用户上，实现对用户的授权（这一过程由PMI体系完成）；其二，通过授权系统由资源的所有者或管理者将一定的角色赋予资源形成授权状，即通过表明哪些角色对特定的资源具有访问权限来实现对资源的授权。利用角色信息将两次授权的结果相关联就得到访问控制列表（ACL），从而实现用户到资源的访问控制。

3.4 密码系统

密码系统是安全应用支撑平台的核心组件。密码系统在独立可信的计算环境中运行，为本地业务系统提供统一的密码服务和信任服务。密码服务提供数据的加密、解密、数字指纹等服务，可以有效保证政务信息传输中的保密性和完整性，以及敏感信息的安全存储；信任服务提供签名、验签和时间戳等服务，为政务系统提供信息的可认证性和抗抵赖性。

3.5 适配系统

当大量用户在平台上工作时，就需要考虑平台的效率问题，否则安全平台就会成为整个电子政务系统的瓶颈。效率问题的解决方法之一是在安全应用平台中加入适配系统。适配系统的基本功能是将位于安全支撑平台上的远程证书信息同步到本地来。

适配系统要做到3个同步。第一，数字证书同步，即将CA的有效证书同步到本地来；第二，属性证书同步，即将AA的有效证书同步到本地来；第三，策略证书同步，即将PA的有效证书同步到本地来。各种证书同步到本地后，就可在本地完成证书的验证，从而提高平台的工作效率。

4 政务信息安全平台的特点

4.1 信任服务与授权服务有机结合

在一般的商务信任服务系统中，由于通常的商务活动仅需参与各方确认相互的身份就可以进行后续的全部操作，信任服务体系与授权服务体系的结合不是十分紧密。相比之下，电子政务领域中每个具体的信任域和特定的管理职能和管理权限的分配机制相对应，这就使得信任服务与相应的授权服务结合得相当紧密，信任服务体系就需要与授权服务体系有机地结合起来。两个体系的结合点就是实现数字证书和属性证书的绑定（见图4）。

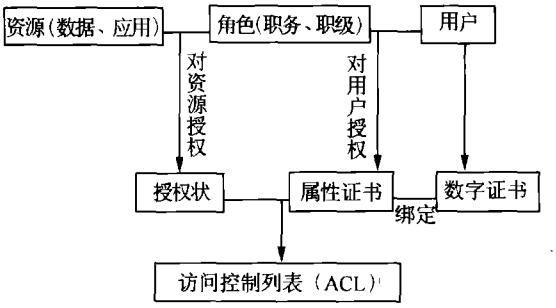

图4　基于角色授权的资源访问控制

4.2 策略服务

与一般的PKI应用系统不同的是，在电子政务PKI系统中有策略服务。策略服务通过PA发放策略证书实现。策略证书不是发放给个人，而是分发给安全应用支撑平台，使平台之间能够用彼此理解的语言进行通信。

在政务系统中，不同的部委与地方使用不同的密码算法，而且，他们运用加密、签名、数字摘要和数字信封等密码服务的先后次序也不尽相同，可能是先加密后签名，也可能是先签名后加密。这样，当数据从一个部门发到另一个部门时，如果不知道发送部门具体使用的密码算法和操作次序，目的部门就无法理解该数据。策略服务体系由策略中心PA及其代理机构PRA组成。PA负责策略的管理并签发策略证书（策略证书描述了使用的密码算法和密码服务的实现次序）。PRA是PA的下设机构，受理审核各机构提出的策略请求。有了策略服务，就可以实现整个政务系统的安全通信。例如，甲地可使用策略有1、2、3，乙地可使用策略有3、4、5，要从甲发信息到乙，先要检查乙是否有相同的策略，两者都有策略3，甲就可以用策略3将信息发送给乙。电子政务安全支撑平台中的策略服务，为灵活、便捷、大规模地部署信息安全平台提供了必要条件。

4.3 证书应用便捷

建立CA、AA，仅仅是可以颁发数字证书和属性证书，要把这些证书投入实际的使用还需要有一个将证书与应用系统相结合的过程。通常的办法是：要么安全开发商把与证书相关的安全函数的接口提供给应用开发商，（下转第88页）

用。共引分析作为一种定量分析方法，结合其他分析方法和专家知识，可以对科技研究活动进行多层次的分析，挖掘数据信息，并利用可视化技术形象表达所得到的知识，从而为政府决策者、科研部门和企业的技术管理者和科研工作者提供有效的决策支持。

参考文献

1 赵党志. 共引分析——研究学科及其文献结构和特点的一种有效方法. 情报杂志，1993(5)

2 Small, H. Macro-level changes in the structure of co-citation clusters: 1983 - 1989. Scientometrics, 26(1): 5 - 20, 1993

3 Small, H. Visualizing Science by Citation Mapping, Journal of the American Society for Information Science. 50(9): 700 - 813, 1999

4 Small, H. A passage through science: crossing disciplinary boundaries. Library Trends, 48(1): 72 - 108, 1999

5 Tsay, Ming-yueh; Wu, Chia-wen; Xu, Hong. Journal co-citation analysis of semiconductor literature. Scientometrics, 57(1): 7 - 25, 2003

6 Chinchilla-Rodriguez, Zaida; Corera-Alvarez, Elena; Herrero-Solana, Victor. A New technique for building maps of large scientific domains based on the cocitation of classes and categories. Scientometrics, 61(1): 129 - 145, 2004

7 Small, H. Paradigms, citations, and maps of science: a personal history. Journal of the American Society for Information Science and Technology. 54(5): 394 - 9, 2003

8 Markus Gmur. Co-citation analysis and the search for invisible colleges: A methodological evaluation. Scientometrics, 57(1): 27 - 57, 2003

9 Small, H; Sweeney, E. Clustering the Science Citation Index using co-citations: 1-A comparison of methods. Scientometrics, 7(3 - 6): 391 - 409, 1985

10 Small, H; Sweeney, E; Greenlee, E. Clustering the Science Citation Index using co-citations: 2-mapping science. Scientometrics, 8(5 - 6): 321 - 340, 1985

11 Rees-Potter; Lorna K; Ress-Potter, L K. Dynamic thesaural systems: a bibliometric study of terminological and conceptual change in sociology and economics with application to the design of dynamic thesaural systems. Information Processing and Management, 25(6): 677 - 691, 1989

12 Gmur, Markus. Co-citation analysis and the search for invisible colleges: a methodological evaluation. Scientometrics, 57(1): 27 - 57, 2003

13 Yulan He, Siu Cheung Hui. Mining a Web Citation Database for author co-citation analysis. Information Processing and Management, 38(4): 491 - 508, 2002

14 Faba-Perez, Guerrero-Bote, De Moya-Anegon. Data mining in a closed Web environment. Scientometrics, 58(3): 623 - 640, 2003

15 Small, H. A general framework for creating large scale maps of science in two or three dimensions: the SciViz system. Scientometrics, 41(1 - 2): 125 - 133, 1998

王建芳 中国科学院文献情报中心，中国科学院研究生院情报学专业2004级博士研究生。通信地址：北京市海淀区中关村北四环西路33号。邮编100080。

冷伏海 教授，中国科学院文献情报中心博士生导师，情报研究部副主任。通信地址同上。

（来稿时间：2005 - 04 - 13）

（上接第55页） 由应用开发商把需要的安全逻辑（如加密、签名、时间戳等）写到业务逻辑中，要么由安全开发商对原来的应用做二次开发，加入安全逻辑。这一过程费时费力，给证书的应用造成了不便。采用安全应用支撑平台代理完成所有的加密、签名等安全事务，可以将安全逻辑从业务逻辑中分离出来，做到证书的应用基本与应用开发无关。这样，安全应用支撑平台就为数字证书的便捷应用创造了条件。

参考文献

1 国家信息安全工程技术研究中心. 电子政务总体设计与技术实现. 北京：电子工业出版社，2003

2 马朝斌. 大力加强电子政务内网的安全保密建设和管理. 信息安全与通信保密，2003(12)

3 谭兴烈. 电子政务安全解决方案要解决的主要问题. 信息安全与通信保密，2004(5)

4 邬贺铨. 电子政务安全体系. 信息安全与通信保密，2003(4)

5 刘远航，崔维利. 电子政务信息安全和PKI/PMI体系. 网络安全技术与应用，2002(7)

6 姜楠，王健. 电子政务中基于PKI的角色授权管理策略. 通信技术，2003(9)

7 许长枫，刘爱江，何大可. 基于属性证书的PMI及其在电子政务安全建设中的应用. 计算机应用研究，2004(1)

李 纲 武汉大学信息管理学院教授。通信地址：武汉。邮编430072。

王毅彦 武汉大学信息管理学院博士研究生。通信地址同上。

（来稿时间：2005 - 04 - 25）