DOI：10.7500/AEPS20130629002

基于 SM2 密码体系的电网信息安全支撑平台开发

骆 钊[1]，谢吉华[1,2]，顾 伟[1]，徐 芳[2]，金钧华[2]
（1. 东南大学电气工程学院，江苏省南京市 210096；2. 无锡市信息安全工程技术研究中心，江苏省无锡市 214001）

摘要：针对电力二次系统安全防护体系缺乏集中管理和审计，且现有的安全体系公钥算法均采用 RSA 算法的现状，提出了基于国产 SM2 密码体系的安全支撑平台的设计和实施方案。分析了安全支撑平台应用 SM2 算法存在的问题，提出了一个采用组件技术构建自行研制的安全加密通道的方案，使得安全支撑平台能支持实现 SM2 算法，并对集成整合后的安全支撑平台的应用功能进行了测试分析。结果表明，该平台可以实现电力二次系统应用之间的无缝整合，使它们相互间形成一个有机整体，提供安全的身份认证、有效的访问控制与权限管理、安全审计日志记录，并对用户信息及系统资源进行管理服务，实现对用户身份和访问权限的集中管理和控制。该平台已在某省级电网正式投运，得到了实际工程应用的验证。

关键词：电力二次系统；SM2 算法；安全支撑平台；组件技术

0 引言

电力二次系统是指各级电力监控系统和调度数据网络以及各级管理信息系统和电力数据通信网络构成的大系统[1]，也是电力异构二元复合网络的关键节点。当电力信息网受到有意或者无意攻击时，信息网的故障可能会通过电力二次系统穿越信息网边界，波及电力物理网，进而导致故障在电力网出现连锁反应，在一些极端情况下，故障在两者之间交替传播，严重威胁电网安全运行[2]。

随着电力二次系统安全防护系统工作的深入开展，众多学者在安全防护体系方面做了大量的研究工作[3-6]。然而，现行支撑电力信息网的电力二次系统都具有自己的安全防护体系，对用户身份认证、资源授权、安全审计、用户管理等难以统一。一方面，当用户角色以及资源需要改变时，电力公司业务运作变得不够顺畅，导致业务流程被割裂，需要过多的人工介入，效率下降，数据一致性降低，使电力二次应用系统失去了应有的作用。另外一方面，安全防护体系公钥算法大多采用 RSA 算法。随着全球范围内密码技术的发展和计算能力的提升，现有的基于 1 024 bit 的 RSA 算法的密码体系已不能满足当前和今后的安全应用需求，尽管增加 RSA 算法密钥长度可以提高原有系统的安全性，但是密钥长度的增加会导致加解密速度降低、硬件实现复杂、基于 RSA 的传输协议在实际应用中存在不可忽视的时延，影响了服务质量[7]，除此之外，欧美等国也限制密钥长度大于 1 024 bit 的 RSA 程序出口。全面采用国产通用算法，这是国家的要求，建立和发展基于国产通用算法的商用密码支撑体系和应用体系是关系国家信息安全的重要措施。2011 年国家密码管理局下发了《关于做好公钥密码算法升级工作的函》（国家密码管理局函〔2011〕7 号），规定 2011 年 7 月 1 日以后投入运行并使用公钥密码的信息系统应使用 SM2 算法；同时，规定从 2011 年 2 月 28 日起在建和拟建公钥密码基础设施的电子认证系统和密钥管理系统应使用 SM2 算法，新研制的含有公钥密码算法的商用密码产品必须支持 SM2 算法，实现 SM2 算法逐步取代 RSA 算法，建立基于国产算法的密码支撑体系。因此，针对电力公司这种关系国计民生、社会稳定的企业，更加需要采用国产算法密码支撑体系，增强电力信息网的安全，防止有害信息和恶意攻击对电力网的干扰而引发的重大生产事故，保证电力生产和调度自动化系统的安全运行。

为此，本文提出了一种基于 SM2 算法密码体系的安全支撑平台的设计和实现方案。由于当前处于 RSA 算法向 SM2 算法过渡的时期，为了节约用户的硬件投资，减少系统的管理工作量，该平台同时支持 RSA 和 SM2 两种算法的密码体系混合使用，这样既不影响现有的业务，又可以满足政策的要求，并

收稿日期：2013-06-29；修回日期：2013-10-25。
国家发改办高技（〔2012〕1424）国家信息安全专项“基于国产加密芯片的加密 U 盘及其软件系统”；江苏省经信委综合（〔2011〕1178）资助项目“加密存储介质及其软件系统的研发和应用”；无锡市 2012 科技支撑项目（CGE01G1211）。

逐步淘汰 RSA 算法的密码体系,最终符合国家密码管理局密码管理规范的要求。基于该方案设计开发的安全支撑平台已经在某省级电网成功投入应用。

1 椭圆曲线加密

椭圆曲线密码学(elliptic curve cryptography,ECC)是基于椭圆曲线离散对数问题的一种公钥密码算法[8],国产 SM2 算法是具有中国自主知识产权并由国家密码管理局发布的公钥密码算法,是 ECC 算法的一种[9]。相对于 RSA 算法,SM2 算法具有以下优点[10]:①安全性能提高,160 bit 的 SM2 算法的安全性与 1 024 bit 的 RSA 算法相当,而 210 bit 的 SM2 算法的安全性则与 2 048 bit 的 RSA 算法相当;②在速度方面,不论是在密钥生成、认证及密钥协商方面,SM2 算法相比 RSA 算法都有非常突出的优势;③存储空间小,SM2 算法的密码一般为 192~256 bit,RSA 算法的密码一般需要为1 024~4 096 bit;④国产算法,无国外可利用的后门。SM2 算法和 RSA 算法的安全性能和速度性能如表 1 和表 2 所示,其中破译所需时间的单位年表示运算速度为 10^6 次/s 的计算机连续运行一年。

表 1 SM2 算法和 RSA 算法的安全性能
Table 1 Security performance of RSA algorithm and SM2 algorithm

破译所需时间/年	密钥长度/bit		密钥长度之比
	RSA 算法	SM2 算法	
10^4	512	106	5∶1
10^8	768	132	6∶1
10^{12}	1 024	160	7∶1
10^{20}	2 048	210	10∶1
10^{78}	21 000	600	35∶1

表 2 SM2 算法和 RSA 算法的速度性能
Table 2 Speed performance of RSA algorithm and SM2 algorithm

算法	签名速度/(次·s^{-1})	验签速度/(次·s^{-1})
256 bit 的 SM2	4 095	871
1 024 bit 的 RSA	2 792	51 224
2 048 bit 的 RSA	455	15 122

为了提高电力二次系统认证平台的安全性,现行的及下一代认证平台和密钥管理系统必须使用国产 SM2 算法。下文涉及的加密设备(USBKey 及加密卡)中都内置 SM2 算法,实现对用户身份的认证,杜绝密钥在客户端内存中出现的可能性。

2 安全支撑平台的设计

针对电力二次系统缺乏集中管理和审计,本文设计了一种安全支撑平台,通过在电力二次系统之前部署一个这样的安全支撑平台作为应用网关,由平台提供安全可靠的身份认证、严格有效的访问控制与权限管理以及进行安全审计日志记录,并对用户信息及系统资源进行管理等功能。安全支撑平台系统结构和部署如图 1 所示。图中所示的轻量目录访问协议(LDAP)数据库用来存取用户信息和访问控制策略信息;①,②,③分别表示可信的第三方证书授权中心(CA)为用户、管理员和安全支撑平台颁发公钥证书;④表示安全支撑平台身份认证模块查询用户信息;⑤表示安全支撑平台授权管理模块查询用户角色信息;⑥表示安全支撑平台安全审计模块查询用户访问日志信息;⑦表示安全支撑平台资源管理模块查询电力二次系统的资源域等相关信息。

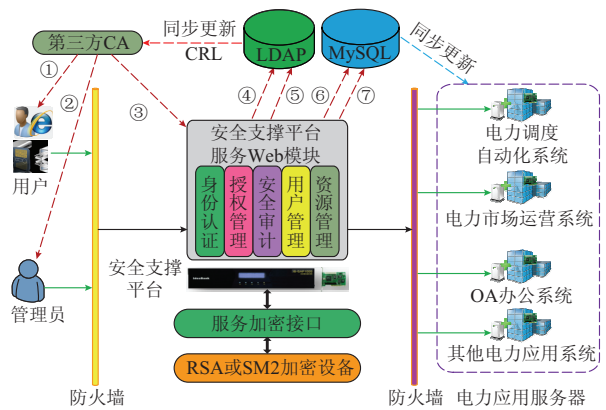

图 1 安全支撑平台系统结构和部署图
Fig.1 Structure and outline of security support platform

用户通过电力信息网访问电力二次系统应用服务时,首先要通过安全支撑平台的身份认证并根据用户角色确定其访问权限后,才能访问相应的电力二次系统应用服务。系统管理员通过电力信息网来配置安全支撑平台和用户信息,完成添加、删除用户等操作,第三方 CA 为用户、管理员和服务器颁发公钥数字证书(PKC),并提供证书撤销列表(CRL)服务。LDAP 数据库一方面为安全支撑平台提供用户信息和访问控制策略,另一方面实时更新 CRL 以确保用户身份的有效性。MySQL 数据库一方面存储审计日志以及各个电力二次系统应用授权码等相关信息,另一方面实时更新应用授权码等信息,确保电力二次系统与用户身份映射的有效性。

安全支撑平台应用 Web Services 技术将身份认证、授权管理、安全审计及用户管理等功能封装为 Web 服务[11],利用 LDAP 数据库存储的用户身份、角色和访问控制等信息和 MySQL 数据库存储安全审计日志以及各个电力应用系统的信息,方便电力

二次应用系统的整合集成调用,从而实现统一认证、统一管理、统一授权和统一审计。

3 安全支撑平台中 SM2 算法的应用

3.1 存在的问题

上述构建的安全支撑平台要支持国家商用 SM2 算法的数字证书,需要考虑两个方面的内容[12],即电力公司的公钥基础设施(PKI)系统是否可以发放支持 SM2 算法的数字证书,以及电力二次应用系统是否可以使用支持国家商用 SM2 算法的数字证书。对于是否可以发放支持国家商用 SM2 算法的数字证书,主要与可信第三方 CA 中心关联;对于是否可以使用支持国家商用 SM2 算法的数字证书,主要与数字证书和电力系统应用业务的整合集成相关。

1)电力公司 PKI 系统是否可以发放支持 SM2 算法的数字证书。目前根据国家商用密码建设来看,支持 SM2 椭圆曲线算法的加密卡和 USBKey 以及加密设备的标准调用接口、证书格式等相关的标准规范基本制定完成,对于发放支持 SM2 椭圆曲线算法的数字证书的条件已完全具备。

2)电力二次系统是否可以使用支持国家商用 SM2 算法的数字证书。现有基于 RSA 算法的安全支撑平台与电力应用系统集成整合,可以细分为客户端和服务器端两个部分:①对于客户端而言,应用环境是基于浏览器/服务器(B/S)架构,用户通过 IE 浏览器访问系统资源时,通过调用 Microsoft 定义的加密应用程序接口(CryptoAPI)调用加密服务提供者(CSP)组件接口,对客户端 USBKey 硬件加密设备进行调用,实现客户端的加密、解密、签名、验证等操作;②对于服务器端(安全支撑平台或电力二次应用系统)而言,其 Web 服务器(例如 Apache、互联网信息服务(IIS)等)可以通过安全套接层(SSL)协议与客户端实现传输信息的加解密,间接地实现身份认证,服务器一般调用标准的 PKCS#11 接口实现硬件加密卡的访问,提供加密、解密、签名、验证的服务。然而 CSP 和 PKCS#11 两类标准的接口中每个密码算法均是以国际标准化组织(ISO)建立的对象标识符(OID)值来进行区分,应用系统通过传递不同的 OID 值对不同的密码算法进行应用。因为国家密码管理局颁布的 SM2 算法是中国自有算法,加之 Microsoft 的 Windows 操作系统的垄断,SM2 算法还没有被 CSP 和 PKCS#11 等标准接口包容,电力二次应用系统无法利用 SSL 安全传输通道传递算法 OID 值的方式实现对 SM2 算法的调用,使得支持 SM2 算法的数字证书无法直接在上述应用环境中使用,进而给现有安全支撑平台升级实现 SM2 算法带来了相应的困难。表 3 为 RSA 算法、国际 ECC 算法及国产 SM2 算法的 OID 值。

表 3 RSA 算法、国际 ECC 算法和国产 SM2 算法的 OID 值
Table 3 OID value of RSA algorithm, international ECC algorithm and domestic SM2 algorithm

算法	OID 值
RSA	1.2.840.113549.1.1.1
国际 ECC	1.2.840.10045.2.1
国产 SM2	1.2.156.197.1.301

3.2 解决方案

电力二次系统业务资源需要操作系统作支撑,然而主流的办公操作系统是 Microsoft 的 Windows 操作系统。Windows 操作系统目前还不支持 SM2 算法数字证书的 OID 值,所以要求 Windows 操作系统支持中国颁布的 SM2 算法数字证书,使 SM2 算法数字证书得到全面的应用还比较困难。针对 SM2 算法数字证书的特殊性,结合对原有数字证书系统进行少量代码改造的原则,在客户端通过国家密码局颁发的加密设备应用接口规范实现客户端 USBKey 的调用,通过浏览器插件的方式实现接口包的下载,而不再借助 Microsoft 的 CSP 接口或国际 PKCS#11 标准接口。在服务器端,因为 SSL 协议不支持 SM2 算法,如果安全传输通道继续采用 SSL 协议,需要而且只能对 OpenSSL(支持 SSL 协议的一种开源软件库)进行改造,虽然通过改造 OpenSSL 可以实现安全支撑平台升级 SM2 算法数字证书,但是会带来以下两个问题。

1)改造 OpenSSL 需要修改大量源代码,工程量极大,而且这种方案只针对 Apache 架构的服务器,对 IIS 服务器或者其他服务器不适用。

2)基于 SM2 算法的加密卡是国家密码管理局制定的接口标准,OpenSSL 需要调用 PKCS#11 标准接口的加密设备,因此,需要对加密接口进行相应的转换,需要相应组件对加密设备进行调用。

鉴于上述情况,加密通道不采用标准的 SSL 协议实现,而是基于组件技术自行设计安全传输通道,实现现有的安全支撑平台升级支持 SM2 算法。通过这种改变调用的方式,从而使电力应用系统可以使用 SM2 椭圆曲线算法的数字证书。

基于组件的开发技术是以嵌入后可立即使用的即插即用型概念为核心,以可重用为目的设计、封装的软件技术[13]。通过采用安全组件技术改变对加密设备的调用方式,完成电力二次应用系统的 PKI

系统升级,实现 SM2 算法的数字证书。下面重点介绍客户端、应用系统及安全支撑平台部署相关安全组件的设计。

3.2.1 客户端的 iMidWare 安全组件

iMidWare 安全组件主要实现对 SJK1134 型 USBKey 进行调用完成用户身份认证,主要功能包括:建立用户端与平台的可信会话,管理用户认证会话及重定向,实现对加密设备的访问。

客户端部署 iMidWare 安全组件之后,客户端如图 2 所示包括 SJK1134 型 USBKey 和 iMidWare 安全组件、浏览器。

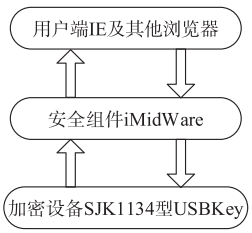

图 2 客户端的组成框图
Fig.2 Block diagram of the client

3.2.2 电力二次应用系统的 iAccount 安全组件

iAccount 安全组件主要实现对 SJK0817-B 型加密卡调用和对访问用户进行身份认证。iAccount 组件为各种电力二次应用系统提供安全可靠的应用接入开发接口,是实现各种异构电力二次应用信息系统的基础。iAccount 组件主要实现建立电力应用服务器与安全支撑平台的可信加密通信,管理用户认证会话及重定向,维护用户认证用户信息,为电力应用系统提供安全审计接口及资源授权接口。

系统管理员将电力应用服务资源映射成应用授权码,并将应用授权码存储于安全支撑平台及电力二次应用系统中,当用户对服务发起访问时,iAccount 组件通过资源授权接口将应用授权码传递给安全支撑平台进行验证,确保授权用户能合法访问。

电力二次应用系统部署 iAccount 安全组件之后,电力二次应用系统如图 3 所示,包括 SJK0817-B 型加密卡、iAccount 安全组件、电力二次应用系统 Web 服务资源。

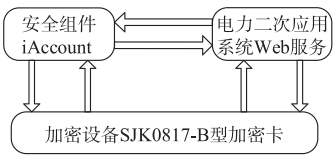

图 3 电力二次应用系统端的组成框图
Fig.3 Block diagram of power secondary application system

3.2.3 安全支撑平台及 iServer 安全组件

iServer 组件是 Web 服务提供者对服务请求者的身份验证的接口程序,是一个能够处理用户访问的底层服务程序模块,主要实现处理用户对计算机或网络资源访问的请求,对用户身份和操作授权进行验证,通过检索资源授权库来决定用户的资源访问权限,同时对用户在电力应用系统中的活动进行行为记录。

部署 iServer 安全组件之后,安全支撑平台如图 4 所示,包括 SJK0817-B 型加密卡、iServer 安全组件、核心服务模块。核心服务模块除了包括 AAAA 服务引擎之外[11],还包括支撑服务程序。支撑服务程序是其他基本功能模块的安全控制程序,负责其他模块之间的调度,同时又是远程网络安全访问的提供者。

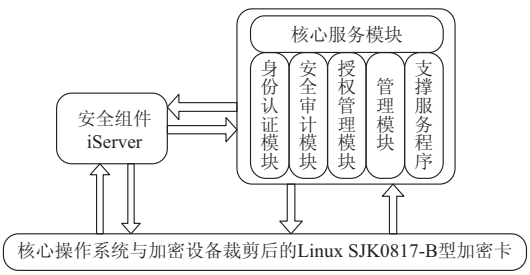

图 4 安全支撑平台的组成框图
Fig.4 Component block diagram of security support platform

3.3 安全支撑平台的升级

采用 SM2 算法的安全支撑平台进行单点登录设计时,通过客户端浏览器部署 iMidWare 组件,安全支撑平台部署 iServer 组件,电力二次应用系统部署 iAccount 组件,实现自行设计安全传输通道替换原有安全支撑平台两个链路上的 SSL 协议加密通道,完成安全支撑平台升级,支持 SM2 算法数字证书。

1)安全支撑平台与客户端的安全传输通道。客户端通过 iMidWare 组件和统一安全支撑平台 iServer 组件,替换这条链路上的 SSL 协议加密通道。两者在安全传输通道进行双向身份认证,安全支撑平台将根据当前用户会话信息、用户基本信息、随机序列值等生成一次性凭证票据,由安全支撑平台证书签名后传递给用户端 iMidWare 安全组件。

2)安全支撑平台与电力应用系统的安全传输通道。为了达到平台升级支持 SM2 算法,在安全支撑平台与电力应用系统分别部署 iServer 组件和 iAccount 组件,电力应用系统调用 iAccount 安全套

件的证书认证接口来首先验证一次性凭证签名的合法性以及应用授权系统授权码的合法性。验证通过，安全支撑平台将用户属性信息和应用扩展信息（如账号、组织、单位等）签名加密后返回给电力二次应用系统。

基于 SM2 算法的安全支撑平台的架构及访问流程如图 5 所示。

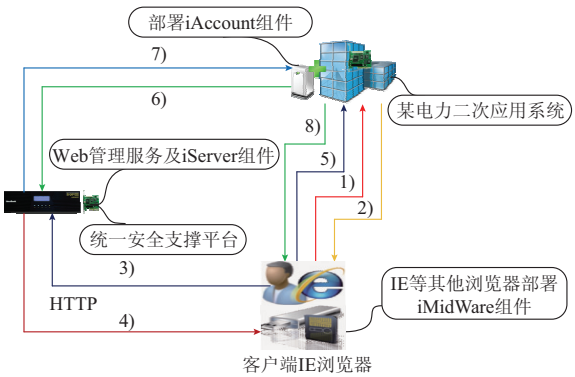

图 5　基于 SM2 算法的安全支撑平台的架构及访问流程图

Fig.5　Architecture and access flow chart of security supporting platform based on SM2 cryptosystem

1）访问用户在客户端插入带 SM2 算法的 USBKey，通过 HTTP 协议及数字证书登录电力二次系统，发起对电力二次系统的访问。

2）电力二次系统服务器调用 iAccount 套件证书，认证接口判断此访问是否经过认证，如没有通过认证，通知客户端的 iMidWare 组件自动重定向至安全支撑平台。

3）安全支撑平台将根据提交的 SM2 算法数字证书验证用户，检查 CRL、证书有效性、用户角色、用户权限等信息，并在认证日志中记录用户名、IP 地址、时间、电力二次系统名称、登录方式、认证状态等信息。

4）SM2 算法数字证书认证通过后，安全支撑平台将根据当前用户会话信息、用户基本信息、随机序列值等由服务器证书签名生成一次性凭证，传递给客户端。

5）客户端通过 iMidWare 组件自动重定向客户端至电力二次系统，并提交这个一次性签名凭证。

6）iAccount 套件证书认证接口首先验证一次性签名凭证，验证通过以后，将应用授权码和一次性签名凭证传递给安全支撑平台，以验证当前会话用户访问签名凭证的合法性以及电力二次应用系统授权码的正确性。

7）验证通过后，安全支撑平台获取用户信息并进行加密，将加密用户信息签名后返回给电力二次应用系统，随即销毁一次性签名凭证。应用系统得到签名的用户信息后，验证该信息的真实性，通过后，解密用户信息，然后根据该用户信息登录电力二次系统。

8）确认用户身份，允许用户正常访问。

4　集成应用及功能测试

该平台已在多个某省级电网投入运行，下面以为电网公司的电力营销支撑系统（包括营销信息管理系统、客户服务管理系统、营销质量管理系统、营销决策支持系统等）及周边的其他电力应用信息系统（负荷管理信息系统、能量采集系统等）构建“大营销”背景下的电力营销综合应用平台为例，说明安全支撑平台是如何在实际应用中解决多个电力信息系统集成问题，并对集成整合后的电力营销综合应用平台进行前后台功能测试。

电网公司的营销支撑系统及周边信息系统按照图 5 所示，分别调用 iAccount 组件接口，实现营销支撑系统及周边异构信息系统集成，完成电力营销综合应用平台的建设。构建的电力营销综合应用平台如图 6 所示。

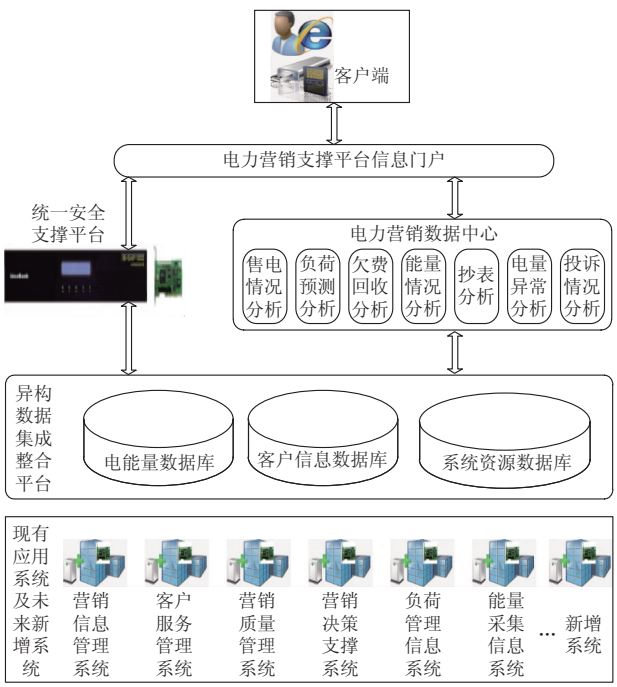

图 6　电力营销综合应用平台的体系结构

Fig.6　Architecture of power marketing integrated application platform

4.1　集成整合前台登录测试

本文是基于数字证书的认证方式对访问用户进

行身份认证,对电力营销综合应用平台进行前台登录测试,主要是验证访问合法用户是否能正常登录电力营销综合应用平台、防止非法用户进入,验证是否可以实现SM2数字证书的认证方式和用户在登录及操作时产生的用户信息能否正常保存在数据库中。通过获取链路中数字证书的公钥参数值,即OID值1.2.156.197.1.301(如附录A图A1所示),说明构建的电力营销综合应用平台可以升级实现SM2数字证书认证方式。

4.2 安全支撑平台功能测试

安全支撑平台借助于Web方式,对平台的身份认证、授权管理、安全审计、用户管理等功能进行测试,验证是否达到预期设计的安全应用需要。

4.2.1 后台登录测试

安全支撑平台的后台登录测试主要包括对合法用户的正常识别和杜绝非法用户,其认证的Web界面如附录A图A2所示。通过查看平台的审计中心的访问认证日志(如附录A图A3所示),用户在访问电力应用系统或者安全支撑平台时,必须先通过安全平台的认证,才能对相应的资源进行访问和操作。

4.2.2 授权管理测试

安全支撑平台的授权管理测试包括资源域的添加、资源域的编辑、资源域状况等内容。授权管理通过管理员对用户角色添加资源域,实现资源的访问权限控制,其授权的Web界面如附录A图A4所示,对用户授权的资源经测试用户能正常访问,反之则不能访问。

4.2.3 安全审计测试

安全支撑平台的安全审计功能测试主要包括查看和管理访问认证、资源授权等日志功能。经测试合法的安全审计员可以查看访问用户对系统资源的访问情况或管理员对用户授权管理情况等日志,而非审计人员不能操作安全审计中心的任何资源,进而无法篡改审计日志。附录A图A3描述了访问认证日志情况,图A5描述了资源授权日志情况。

4.2.4 用户管理测试

安全支撑平台用户管理功能测试主要包括对角色管理、用户组管理及用户信息管理功能进行测试,用户管理员通过角色管理模块为系统管理员提供增加新角色、删除角色、修改现有角色的描述等操作。

实践表明,安全支撑平台为电力二次系统安全防护监管提供了有效的技术手段。一方面,运行人员可以通过安全支撑平台全面掌握电力二次系统安全状态,及时发现安全隐患;另一方面,安全支撑平台为电力二次系统提供了完备的、标准化的基础信息,便于进行安全审计。

5 结语

通过统一安全支撑平台,将每个区目前分散的各个电力二次应用系统进行异构集成整合,实现用户统一身份认证、统一管理和统一授权以及统一审计,既能有效地保护电力二次应用系统又极大地简化了应用中访问控制和权限管理系统的开发与维护,并减小了管理成本和降低了复杂性。其次,本文采用国产SM2公钥算法,安全性更高,保证国家层面上的信息安全。因此,本设计既满足了电力二次系统的安全管理,又实现了信息安全产品的国有化,具有重要的现实意义。

附录见本刊网络版(http://aeps.sgepri.sgcc.com.cn/aeps/ch/index.aspx)。

参考文献

[1] 胡炎,辛耀中,韩英铎.二次系统安全体系结构化设计方法[J].电力系统自动化,2003,27(21):63-68.
HU Yan, XIN Yaozhong, HAN Yingduo. A method for the structured security architecture design of secondary systems[J]. Automation of Electric Power Systems, 2003, 27(21): 63-68.

[2] 梅生伟,王莹莹,陈来军,等.从复杂网络视角评述智能电网信息安全研究现状及若干展望[J].高电压技术,2011,37(3):672-679.
MEI Shengwei, WANG Yingying, CHEN Laijun, et al. Overviews and prospects of the cyber security of smart grid from the view of complex network theory [J]. High Voltage Engineering, 2011, 37(3): 672-679.

[3] 刘刚,梁野,李毅松,等.数字证书技术在电力二次系统中的实现及应用[J].电网技术,2006,30(增刊1):71-75.
LIU Gang, LIANG Ye, LI Yisong, et al. Realization and application of certificate in secondary part power system [J]. Power System Technology, 2006, 30(Supplement 1): 71-75.

[4] 王保义,杨丽.基于安全网关的电力二次系统安全防护[J].电力系统通信,2008,29(19):28-32.
WANG Baoyi, YANG Li. Security protection of power secondary system based on security gateway[J]. Telecommunications for Electric Power System, 2008, 29(19): 28-32.

[5] 秦超,张涛,林为民.基于数字证书认证的电力安全拨号认证系统[J].电力系统自动化,2009,33(19):52-55.
QIN Chao, ZHANG Tao, LIN Weimin. A digital certificate authentication based electric power safe dialing authentication system [J]. Automation of Electric Power Systems, 2009, 33(19): 52-55.

[6] 余勇,林为民,何军.电力数字证书服务系统的设计及应用[J].电力系统自动化,2005,29(10):64-68.

YU Yong, LIN Weimin, HE Jun. Design and application of power digital certificate service system[J]. Automation of Electric Power Systems, 2005, 29(10): 64-68.

[7] 游韵,喻占武.基于椭圆曲线公钥算法的SSL协议分析和实现[J].微计算机信息,2006,22(30):213-215.
YOU Yun, YU Zhanwu. Analysis and implementation of SSL protocol based on elliptic curve cryptosystem[J]. Microcomputer Information, 2006, 22(30): 213-215.

[8] AMARA M, SIAD A. Elliptic curve cryptography and its applications[C]// 7th International Workshop on Systems, Signal Processing and Their Applications (WOSSPA), May 9-11, 2011, Tipaza, Algeria: 247-250.

[9] 国家密码管理局.SM2椭圆曲线公钥密码算法[EB/OL].[2013-04-26]. http://www.oscca.gov.cn/UpFile/2010122214822692.pdf.2010-12-17/2011-12-08.

[10] 张险峰,秦志光,刘锦德,等.椭圆曲线加密系统的性能分析[J].电子科技大学学报,2001,30(2):144-147.
ZHANG Xianfeng, QIN Zhiguang, LIU Jinde, et al. Analysis of security and efficiency on elliptic curves cryptosystems[J]. Journal of University of Electronic Science and Technology of China, 2001, 30(2): 144-147.

[11] 骆钊,金均华,谢吉华.基于PKI/PMI的AAAA服务器在电力系统信息安全中的应用研究[J].电力信息化,2012,10(12):87-91.
LUO Zhao, JIN Junhua, XIE Jihua. Applied research of PKI/PMI based AAAA server for power system information security[J]. Electric Power Information Technology, 2012, 10(12): 87-91.

[12] 黎满贵.PKI系统支持SM2椭圆曲线公钥密码算法的研究[J].信息安全与通信保密,2011,9(9):78-80.
LI Mangui. Study on public key infrastructure in support of public key cryptographic algorithm SM2 based on elliptic curves[J]. China Information Security, 2011, 9(9): 78-80.

[13] 王飞,吴义忠,戴同,等.基于组件技术的工程设计资源库的研究与开发[J].计算机工程与应用,2003,39(31):140-142.
WANG Fei, WU Yizhong, DAI Tong, et al. Design and development of an engineering design resources base system based on component technology[J]. Computer Engineering and Application, 2003, 39(31): 140-142.

骆 钊(1986—),男,通信作者,博士研究生,主要研究方向:微电网优化、电力系统运行与控制、电力系统信息安全。E-mail: waiting.198611@gmail.com

谢吉华(1964—),男,副教授,主要研究方向:电力系统信息安全和智能仪器。

顾 伟(1981—),男,博士,副教授,博士生导师,主要研究方向:智能电网、可再生能源接入技术及电能质量分析控制。E-mail: wgu@seu.edu.cn

(编辑 蔡静雯)

SM2-Cryptosystem Based Information Security Supporting Platform in Power Grid

LUO Zhao[1], *XIE Jihua*[1,2], *GU Wei*[1], *XU Fang*[2], *JIN Junhua*[2]

(1. School of Electrical Engineering, Southeast University, Nanjing 210096, China;
2. Wuxi Information Security Engineering Technology Research Center, Wuxi 214001, China)

Abstract: The security protection system of the secondary power system has no central management and auditing, and the public key algorithm of existing security systems is RSA algorithm. So a design and implementation scheme for security supporting platform based on domestic SM2 cryptosystem is proposed. First, the difficulty in making the security supporting platform upgraded to support the SM2 algorithm is pointed out. Then a scheme of building the self-developed security encrypted channel with the component technology is proposed to ensure the SM2 algorithm can be realized in the security supporting platform. Finally, the application function of integrated security supporting platform is tested and analyzed. The results show that this platform can achieve smooth integration among the applications of the secondary power system, while providing safe identity authentication, effective access control and authorization management, safety auditing logging, and user management. What's more, the security support platform can centralize the identity authentication and the access control. The platform has been applied in a certain provincial power grid, which has proved its availability in actual projects.

This work is supported by National Information Security Special Program from National Development and Reform Commission (No. (2012)1424), Jiangsu Provincial Economic and Information Commission (No. (2011)1178), and Wuxi City Technology Research and Development Program 2012 (No. CGE01G1211).

Key words: power secondary system; SM2 algorithm; security supporting platform; component technology