

# 密钥管理系统研究与实现

陈亚东,张 涛,曾 荣,费稼轩,华 晔,叶 云

(中国电力科学研究院,江苏 南京 210003)

**摘 要:**密码技术是信息安全问题的核心技术之一,密钥管理技术是密码技术的基础,在密钥的产生、存储、分配、更新、吊销、控制、销毁等密钥全生命周期过程中保证密钥的安全,保证对称密钥和非对称密钥的有效和安全管理,并提供高效、经济的密钥服务十分关键。文中从基础设施层到系统的管理层设计了将对称密钥和非对称密钥在整体上统一管理的密钥管理系统,实现了对密码设备的实时安全监控,可以作为一个独立提供对称密钥和非对称密钥全生命周期安全管理服务的密钥管理系统,也可以扩展作为数字证书发布系统的密钥管理系统后台。

**关键词:**密码技术;密钥管理;非对称密钥;对称密钥

中图分类号:TP302.1

文献标识码:A

文章编号:1673-629X(2014)02-0156-04

doi:10.3969/j.issn.1673-629X.2014.02.038

## Research and Implementation of Key Management System

CHEN Ya-dong, ZHANG Tao, ZENG Rong, FEI Jia-xuan, HUA Ye, YE Yun

(China Electric Power Research Institute, Nanjing 210003, China)

**Abstract:** Cryptographic technology is one of the core technologies of information security, which is basis of key management. To provide efficient and economic key service, it is of crucial importance to ensure the safety of secret key throughout the process of the whole life cycle includes system initialization, key generation, key encasement, key distribution, key storage, key renovation, key destruction, and to assure the effective and safety management of symmetric key and asymmetric key. Describe the design of key management system from the infrastructure layer to the management layer, the system provides real-time safety monitoring of cryptographic devices, key management system can be used as an independent with a symmetric key and asymmetric key lifecycle safety management services, also can be extended to be the key provider of CA (Certificate Authority) system.

**Key words:** cryptographic technology; key management; asymmetric key; symmetric key

## 0 引言

随着我国社会的信息和网络化的快速应用与发展,网络安全问题在各行业的信息系统中越来越突出,采用对称密钥和非对称密钥的数据加密技术是保证数据加密通信和身份认证的重要机制。电力、石油、金融等国计民生重要行业,都建立了保证企业信息安全防护的IC卡密钥管理系统、数字证书系统等密钥管理系统,越来越多的行业和部门也意识到信息安全在生产 and 生活中的重要性和紧迫性,认识到基于密码技术的信息安全解决方案是解决信息传输保密的可靠途径。

文献[1-2]描述了基于PKI技术的数字证书系统的实现,描述了证书申请、分发、更新等过程中的密钥安全服务机制,设计了典型的非对称密钥管理系统。文献[3-4]中描述了建立对称密钥管理系统的方案。

以上都是提供单一功能的密钥管理系统,不能同时提供非对称密钥服务和对称密钥服务的综合系统,并没有对密码机的功能有效性和安全性进行监控的机制。

文中在密钥管理关键技术研究的基础上,对密钥管理系统的体系架构、逻辑层次和功能模块做出详细设计,提出将密钥管理工作独立模块化设计,作为一个密钥管理后台的方法,集中为证书管理系统、对称密钥服务系统提供服务,并支持对密码设备的算法有效性检查,设备的在线监控,可以满足既需要对称密码服务,又需要非对称密码服务的行业应用需求。

## 1 总体布局

密钥管理系统设计的总体布局如图1所示,密钥管理系统可以同时提供非对称密钥服务和对称密钥服

收稿日期:2013-05-02

修回日期:2013-08-06

网络出版时间:2013-11-29

基金项目:国家电网科技计划项目(SGKJ-XXTX-2013004)

作者简介:陈亚东(1982-),男,通信作者,硕士,工程师,CCF会员,研究方向为电力系统网络安全技术。

网络出版地址: <http://www.cnki.net/kcms/detail/61.1450.TP.20131129.0857.015.html>

务,可以按照级联模式根据应用需求扩展成二级或者三级对称密钥和非对称密钥管理体系。密钥管理系统也可以按照《数字证书认证系统密码协议规范》,改造证书认证和数字签名中通用的安全协议流程、数据格式和密码函数接口<sup>[5]</sup>,与其他 CA 系统通信,系统本身作为一个非对称密钥库,与 CA 结合形成证书系统,也可以作为对称密钥库,与对称密钥管理系统前台管理系统配合提供对称密钥全生命周期服务<sup>[6]</sup>。

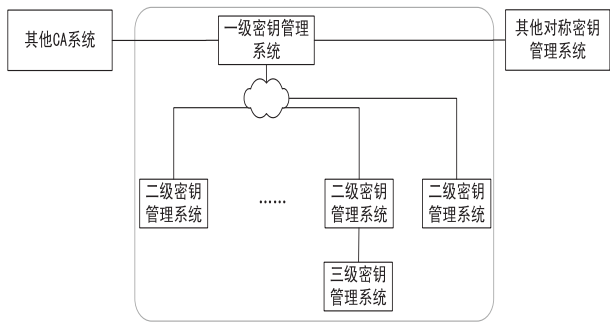


图 1 密钥管理系统总体拓扑

2 逻辑层次

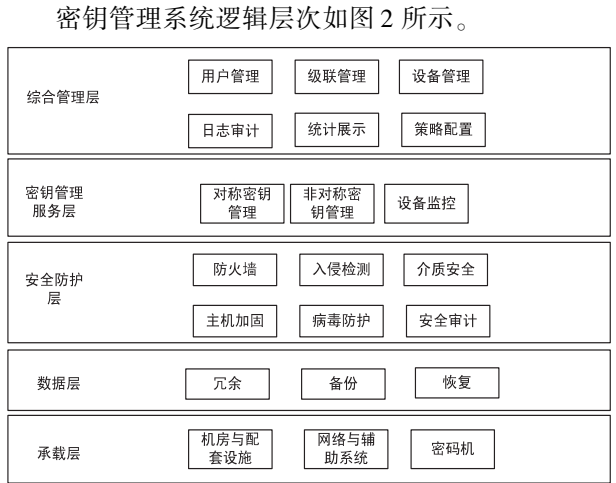


图 2 密钥管理系统逻辑层次

承载层和数据层提供密钥管理系统运行的承载网络及机房与配套设施,为密钥管理系统提供物理运行环境,提供冗余和备份与恢复服务器、备份磁带机、磁盘阵列等密钥的数据存储手段。

安全防护层按照等级保护要求,采用介质安全、防火墙、入侵检测、主机加固、病毒防护、安全审计等技术手段,为密钥管理系统的网络部署提供基本的安全防护手段,保证密钥管理服务的安全。

密钥管理服务层提供核心密钥管理服务,非对称密钥管理和对称密钥管理模块提供非对称密钥和对称密钥的证书模版管理、应用策略管理、密钥全生命周期管理、密钥库管理。设备监控模块在线监测密码设备运行情况,检查密码设备的算法类型、密钥长度、密码设备基本信息(厂商、类型、设备编号、IP 地址)与录入

时是否一致,对密钥管理系统密码设备之间的安全通信协议、密码设备支持算法是否符合国家密码管理局标准规定进行在线监控和异常报警<sup>[7-8]</sup>。

综合管理层保证密钥管理系统支持各级系统管理员经授权后以 B/S 模式对该系统进行全面管理和可视化展示,支持浏览、统计、查询等操作,掌握和了解本级密钥管理系统密钥使用情况、密码设备配用情况和运行情况、密码应用详细信息,支持对该系统的密码设备和拓扑进行管理和展示,支持配置系统操作员、管理员的不同权限,级联模式下可对各级密码设备进行录入、注册、配置、认证及基本信息管理。综合管理层还支持管理员监控操作日志、监控日志和运行日志。

3 系统拓扑

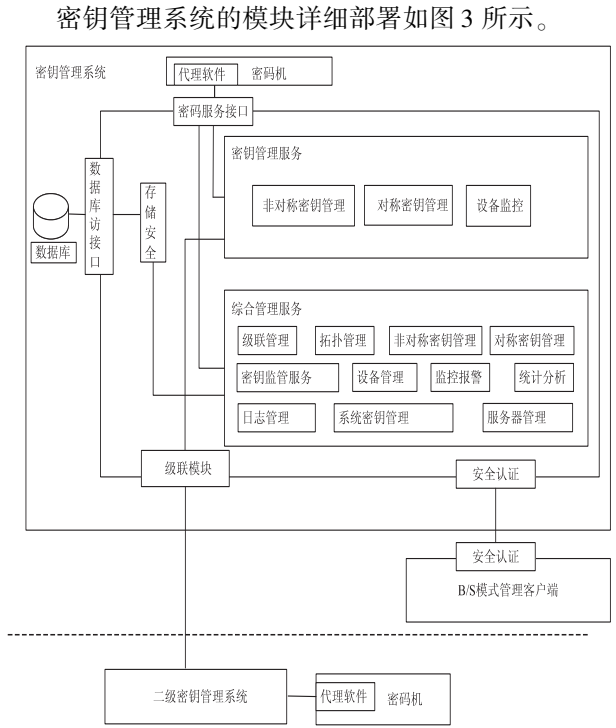


图 3 密钥管理系统模块部署

从图上可以看出,密钥管理系统支持二级和更多级级联,如果系统的密钥管理服务配合密码服务接口与第三方 CA 系统连接,可以作为第三方 CA 的密钥管理中心。系统内部各模块之间通讯直接调用密码机硬件加密算法进行身份认证和数据加密传输,算法模块支持 Windows、JAVA 等各种平台<sup>[9]</sup>。

密码设备监控机制通过在密码机部署的代理软件实现,代理软件针对密码机的操作系统开发,和密钥管理服务的设备监控模块以客户端-服务器方式实现监管<sup>[10]</sup>,密码设备的算法有效性、密码设备基本信息(厂商、类型、设备编号、IP 地址)事先在综合管理平台录入基准值,密钥管理系统运行时,代理软件定期监测密码设备,对密码设备基本信息等固定值的检查通过采

集并比对基准值方式监测。算法有效性的检查通过计算实现,代理软件首先调用密码机取随机值,通过对称密钥、非对称密钥计算,并计算哈希值,形成基准值,和明文一起通过服务端服务器的公钥证书加密发送至设备监控服务端,服务端收到后解密并计算明文哈希值,如果与收到的哈希值相同,说明代理软件所在密码机算法正确,如果不正确则告警<sup>[11-12]</sup>。

设备监控代理软件还支持密钥分发功能,当二级密钥管理系统,例如非对称密钥管理模块需要分发密钥时,综合管理服务模块向下级密码设备的代理软件发起密钥分发通知,代理软件接收通知后,主动连接综合管理服务模块,综合管理服务模块将要分配的密钥下发给代理软件,完成密码设备的密钥分发操作。

4 系统扩展

当密钥管理系统只提供对称密钥和非对称密钥核心密钥管理服务,与其他系统例如 CA 系统整合时,作为密钥管理中心,需要定义非对称密钥管理模块和 CA 模块之间的互联互通密码认证协议<sup>[13]</sup>。

非对称密钥服务包括申请密钥对、恢复密钥对和撤销密钥对,每个服务都按照请求-响应的步骤执行:

请求:请求由 CA 提出,发送到密钥管理系统。CA 在生成用户加密证书、更新加密证书或者撤销加密证书时,首先组织密钥服务请求,发送到密钥管理系统,并延缓自身的事务处理过程,等待密钥管理系统响应返回。

响应:响应由密钥管理系统发起,发送到 CA。密钥管理系统在接收到来自 CA 的请求后,检查确定请求合法性,处理服务请求,并将结果返回给 CA。

整个服务过程如图 4 所示。

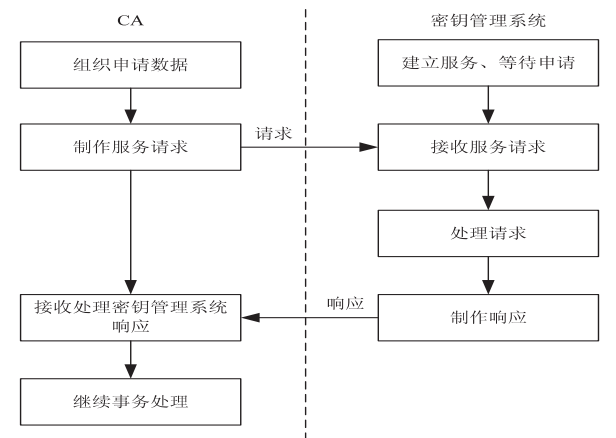


图 4 密钥管理系统与 CA 通讯过程

请求:

密钥服务请求,包含 CA 请求的类型、性质以及特性数据等,该请求将被发送到密钥管理系统并得到服务。服务请求包括如下数据:协议版本、服务请求标识

符、CA 标识符、扩展的请求信息、请求信息的签名<sup>[14]</sup>。

响应:

指密钥管理系统对来自 CA 请求的处理响应。密钥管理系统的响应包括如下数据:协议版本、响应标识符、密钥管理系统标识符、响应信息、响应信息的签名。

CA 请求的基本格式如下:

```
CARequest ::= SEQUENCE {
    ksRequest KSRequest,
    signatureAlgorithm AlgorithmIdentifier,
    signatureValue OCTET STRING
}
```

其中:

```
KSRequest ::= SEQUENCE {
    version Version DEFAULT v2,
    caName EntName,
    requestList SEQUENCE OF Request,
    requestTime GeneralizedTime,
    taskNo INTEGER
}

Version ::= INTEGER { v2(1) }
EntName ::= SEQUENCE {
    hashAlgorithm AlgorithmIdentifier,
    entName GeneralName,
    entPubKeyHash OCTET STRING,
    serialNumber CertificateSerialNumber
}
```

```
Request ::= CHOICE {
    applyKeyReq [0] IMPLICIT ApplyKeyReq,
    restoreKeyReq [1] IMPLICIT RestoreKeyReq,
    revokeKeyReq [2] IMPLICIT RevokeKeyReq
}

RequestTime ::= GeneralizedTime;
```

密钥管理系统响应的基本格式如下:

```
KMRespond ::= SEQUENCE {
    ksRespond KSRespond,
    signatureAlgorithm AlgorithmIdentifier,
    signatureValue OCTET STRING
}
```

其中:

```
TBSRespond ::= SEQUENCE {
    version Version DEFAULT v2,
    KMName entName,
    respondList SEQUENCE OF Respond,
    respondTime RespondTime,
    taskNO INTEGER
}

Version、entName、TaskNo 数据格式在前文已经解释

Respond ::= CHOICE {
    applykeyRespond [0] IMPLICIT RetKeyRespond,
    restorekeyRespond [1] IMPLICIT RetKeyRespond,
    revokekeyRespond [2] IMPLICIT RevokeKeyRespond,
```

```
errorPkgRespond [3] IMPLICIT ErrorPkgRespond
}
RespondTime:=GeneralizedTime;
    密钥管理系统和第三方对称密钥管理系统对接可以
    以采用基于数字组证书技术的身份认证协议互相验证
    对方身份,协议可以采用 SSLv3 模式进行。
```

5 结束语

文中设计了一种同时支持对称密钥管理和非对称密钥管理的密钥管理系统,支持对密码设备的算法有效性和设备基本配置的实时监控,其核心密钥管理模块还支持与第三方 CA 系统和对称密钥管理系统对接,作为 CA 系统和对称密钥管理系统的密钥管理中心服务,是一种采用模块化设计的配置灵活的密钥管理系统。

参考文献:

[1] 刘培顺. 基于 PKI 的密钥管理系统[D]. 成都:西南交通大学,2001.

[2] 刘 颖. 密钥管理基础设施中的非对称密钥管理系统设计[D]. 上海:上海交通大学,2008.

[3] 朱国强. 对称密钥管理体系结构研究[D]. 上海:上海交通大学,2006.

[4] 侯永亮,蔚晓明. 智能电能表密钥管理系统的研究[J]. 山

西电力,2012( Sup ):15-17.

[5] 张燕燕. 电子商务中证书认证系统的设计与实现[D]. 济南:山东大学,2007.

[6] ANSI x9.17( Revised). Americannational standard for financial institution key management[ S ]. 1985.

[7] Ghodosi H, Pieprzyk J, Safavi-Naini R, et al. On construction of cumulative secret sharing schemes [ C ]//Proc of ACISP. [ s. l. ]:[ s. n. ],1998.

[8] Thomas R, Sandhu R. Task-based authorization controls (TBAC):A family of models for active and enterprise-oriented authorization management[ C ]//Proc of eleventh international conference on database security. Lake Tahoe, California, USA:[ s. n. ],1997.

[9] 徐 勇. 基于 PKI 技术的 CA 的研究与实现[D]. 成都:四川师范大学,2007.

[10] 闫鸿滨. 密钥管理技术研究综述[J]. 南通职业大学学报,2011,25(1):79-83.

[11] 郑金涛. 基于 KMS 的直接密钥托管方案的设计与实现[D]. 武汉:华中科技大学,2007.

[12] 郑金涛. 基于密钥管理的密钥分发解决方案探析[D]. 武汉:华中科技大学,2007.

[13] 何映伟,邓小艳,吉庆兵. 一种混合密码体制下的密钥管理方案[J]. 通信技术,2012,45(1):122-124.

[14] 宋 磊,罗其亮,罗 毅,等. 电力系统实时数据通信加密方案[J]. 电力系统自动化,2004,28(14):76-81.

(上接第 155 页)

部分时间,只需对自动化测试的测试数据文件、测试配置文件进行维护。回归测试时,设置必须的测试用例项;在新功能添加时,维护相应的测试数据文件即可,极大地提高了测试人员进行系统回归测试的效率。

4 结束语

文中分析了软件自动化测试技术发展近况,根据项目的要求,对关键字驱动的自动化测试框架进行研究,提出了关键字驱动的自动化测试设计方案,通过实现层次数据文件设计与关键字结构设计,保证了测试业务的灵活配置,实现了测试数据、测试脚本和测试逻辑的分离思想。

参考文献:

[1] 龚 丹. 自动化测试之我见[J]. 计算机光盘软件与应用,2012(17):83-84.

[2] 刘 旭. 软件测试自动化的测试研究[J]. 煤炭技术,2012,31(7):168-169.

[3] Pajunen T,Takala T,Katara M. Model-based testing with a general purpose keyword-driven test automation framework [ C ]//Proc of 2011 fourth international conference on soft-

ware testing, verification and validation. [ s. l. ]:[ s. n. ],2011:242-251.

[4] 夏 晶. 基于 QTP 的功能自动化测试框架的研究与应用[D]. 武汉:武汉科技大学,2010.

[5] 吴显光. 软件自动化测试[J]. 中国新通信,2012,14(14):67-69.

[6] 朱 菊,王志坚,杨 雪. 基于数据驱动的软件自动化测试框架[J]. 计算机技术与发展,2006,16(5):68-70.

[7] 王 君,朱美正,李 欣. 关键字驱动测试框架的研究与实现[J]. 计算机工程与设计,2010,31(10):2246-2248.

[8] Zylberman A,Shotten A. Test language-introduction to keyword driven testing[ C ]//Proc of quality assurance and software testing. [ s. l. ]:[ s. n. ],2010.

[9] Rashmi,Bajpai N. A keyword driven framework for applications[J]. International journal of advanced computer applications,2012,3(3):8-14.

[10] 钱月琴. 关键字驱动框架中关键字划分方法研究[J]. 计算机技术与发展,2010,20(9):44-47.

[11] 黄梦薇,黄大庆,周 未. 基于 WATIR 的 WEB 自动化回归测试框架[J]. 电子设计工程,2012(21):34-36.

[12] 冯玉才,唐 艳,周 淳. 关键字驱动自动化测试的原理与实现[J]. 计算机应用,2004,24(8):140-142.

作者：[陈亚东](#)，[张涛](#)，[曾荣](#)，[费稼轩](#)，[华晔](#)，[叶云](#)，[CHEN Ya-dong](#)，[ZHANG Tao](#)，[ZENG Rong](#)，[FEI Jia-xuan](#)，[HUA Ye](#)，[YE Yun](#)  
作者单位：[中国电力科学研究院, 江苏 南京, 210003](#)  
刊名：[计算机技术与发展](#)



英文刊名：[Computer Technology and Development](#)

年，卷(期)：2014(2)

本文链接：[http://d.wanfangdata.com.cn/Periodical\\_wjfz201402039.aspx](http://d.wanfangdata.com.cn/Periodical_wjfz201402039.aspx)