统一密钥支撑体系的研究

刘金锁,黄益彬,杨维永
(国网电力科学研究院,江苏 南京 210006)

摘 要:随着企业互动化、移动化和智能化业务的逐步推进,密码技术作为业务信息安全保护的核心内容越来越重要,但由于业务系统所采用的密码算法及应用模式的不同,通常企业存在多种多样的密钥管理系统,导致密钥资源无法有效快速利用,缺少统一的密钥监控和保护措施。文中介绍的统一密钥支撑体系以密钥管理 PDCA 为模型,从密钥管理体系及标准,密钥监控与分析系统和密钥安全性检测平台出发构建层次化的体系架构,规范业务系统密码技术的使用方式和流程,完善密钥全生命周期安全管控措施,建立业务系统标准化、通用和统一的密钥检测和评价体系,消除密码应用的安全隐患,保障密钥的安全、可靠以及高效使用,提升企业密钥管理水平。

关键词:密钥管理;密钥检测;生命周期;信息安全
中图分类号:TP393.08 **文献标识码**:A **文章编号**:1673-629X(2014)03-0122-04
doi:10.3969/j.issn.1673-629X.2014.03.031

Research on Unified Key Support System

LIU Jin-suo, HUANG Yi-bin, YANG Wei-yong
(State Grid Electric Power Research Institute, Nanjing 210006, China)

Abstract: With the interactive, mobile and intelligent business step by step, password security protection technology as the core content of business information is becoming more and more important, but because the password algorithm and application mode adopted by business system is different, usually enterprise key management system varied, leading to key resources cannot effectively use, lack of key monitoring and protection measures unified. Unified key support system introduced takes key management PDCA as the model, starting from the key management system and standard, architecture of key monitoring and analysis system and the key safety detection platform construct the hierarchical system, specifying the cryptography application system using methods and processes, improving key lifecycle safety management measures, establishing business system standardization, universal and unified key detection and evaluation system, removing the password application security hidden danger, ensuring the key safe, reliable, and efficient use, enhancing the enterprise key management level.

Key words: key management; key detection; life cycle; information security

0 引 言

随着信息化的大力发展,企业信息系统采用密码技术进行身份认证和数据加密传输的应用越来越广泛,特别是移动化业务的开展,终端智能化的增强,作为身份认证与数据加密传输基础性支撑技术的密码技术在企业信息化建设、运行与管理中发挥了重要作用。密码技术的核心内容是通过加密方法把对大量数据的保护归结为对若干核心参量密钥的保护[1-2],因此业务系统中密钥管理问题就成为首要的核心问题。密钥管理要处理密钥自产生到最终销毁的整个过程的所有问题,包括密钥的产生、存储、备份/装入、分配、保护、更新、控制、丢失、吊销和销毁等[3-4],密钥管理不仅影响系统的安全性,而且涉及到系统的可靠性、有效性和经济性。密码技术的广泛应用为信息系统技术革新提供技术支撑的同时,也对新时期企业信息安全建设提出了新的挑战。

1 密钥管理现状

回顾我国信息化的发展历程,基本上是“从无到有,从有到大,从大到强”的几个阶段,企业信息安全

收稿日期:2013-05-15 **修回日期**:2013-09-08 **网络出版时间**:2014-01-08
基金项目:国家电网公司科技计划项目(SGKJ-XXTX-2013004)
作者简介:刘金锁(1980-),男,山西临汾人,高级工程师,硕士,研究方向为网络信息安全、可信计算。
网络出版地址:http://www.cnki.net/kcms/doi/10.3969/j.issn.1006-2475..html

建设也是伴随着信息化的建设开展的,但整体滞后,特别是作为信息安全基础设施的密钥管理更为落后,缺少整体规划设计,造成密钥管理体系缺失,不同业务系统根据自身的需求建立各自的密钥系统,为各自应用提供密码服务,例如对称密钥管理系统、非对称密钥管理系统[5-6]、金融密钥管理系统等。这些系统各自使用的密钥技术和密码支撑服务各不相同,应用模式差异大,在管理方法、管理流程、管理机制方面缺乏统一的协调机制,业务系统使用不同种类密钥时需要向不同的密钥管理部门申请,管理、控制与监管成本较高[7];同时,企业移动化和互动化业务的开展,大量智能终端、设备和人员应用了海量密钥,但缺乏统一安全技术管控措施,无法对现有密钥的安全状态进行全面的监控和跟踪,一旦出现密钥遭受攻击导致被破解,或者无法实时获取密钥状态等情况,将会造成严重的安全隐患[8-9]。因此迫切需要建立统一的密钥支撑体系,对各类业务系统的密钥应用提供有效的服务与支撑,提升企业密钥生成、存储、使用、更新、废除、归档、销毁、备份和恢复全生命周期的精确感知能力,加强对密钥的合规性和合法性监管[10],消除密码应用的安全隐患,保障密钥的安全、可靠以及高效使用,提升企业密钥管理水平。

2　统一密钥支撑体系架构

2.1　体系模型

统一密钥支撑体系是以密码学中密钥全生命周期管理为理论指导,以管理体系及标准、关键技术和测评技术为主线,重点解决密码相关安全基础设施、业务系统、用户终端等环境下的密钥使用、检测、监控等问题。

建立统一对称及非对称密钥的管理体系及标准,指导企业各项业务在规划、设计、开发、建设及运维过程中密钥规范化的使用;建立密钥安全性检测平台,实现对业务系统标准化、通用、统一的密钥检测和评价体系,确保业务系统的安全性;建立密钥监控与分析系统对密钥的产生、传输、分发、恢复、更新、撤销过程的全生命周期安全管控,实现对密钥合规、合法性进行监管。统一密钥支撑体系的各环节依据信息安全 PDCA(计划-实施-检查-措施)模型设计,具体关系如图 1 所示。

密钥管理体系及标准提供政策、法规及安全性等方面的指导和约束,指导业务系统及密钥基础设施建设。密钥安全性检测平台对业务系统及密钥基础设施进行测试和评价。密钥监控与分析系统对密钥的使用进行监管,对发现的问题及时反馈管理体系不断改进。通过统一密钥支撑体系 PDCA 模型的建设,完善企业信息安全体系并可以持续改进。

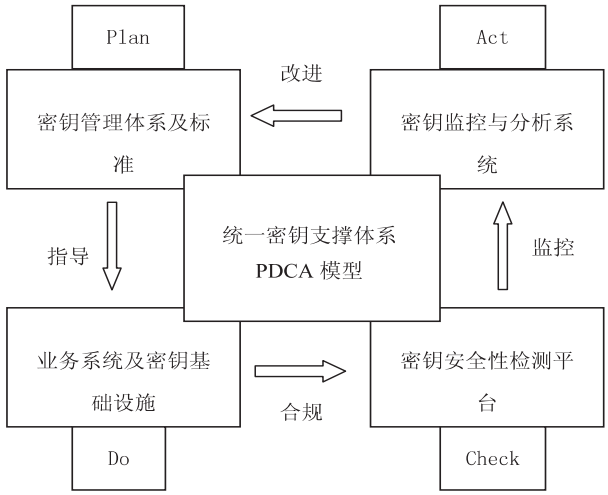

图 1　统一密钥支撑体系 PDCA 模型

2.2　体系架构

统一密钥支撑体系针对对称、非对称密钥及数字证书的应用模式,对密钥管理、密钥支撑技术、密钥监控措施以及密钥检测方法进行层次化设计[11-13],结构上可分为密钥管理体系及标准、密钥监控与分析系统和密钥安全性检测平台,层次化划分如图 2 所示。

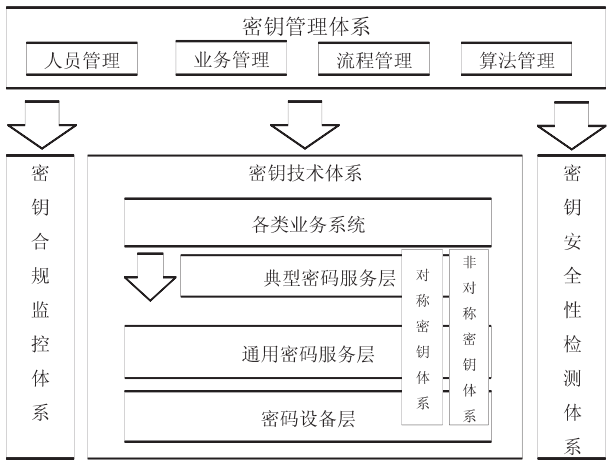

图 2　统一密钥支撑体系架构

密钥管理体系及标准主要包括合规建立人员管理、流程管理、算法管理、业务管理等一系列管理规范。密钥监控与分析系统包括各层应用、设备之间的密钥调用关系,以及合规、合法的使用密钥为上层业务应用系统提供高效、可靠的密码服务,实时监控业务应用、密码设备的运行的合规性、可靠性及实时状态。密钥安全性检测平台对业务应用、密码设备的合规性、密码算法的支持、安全性等指标进行评测。

3　统一密钥支撑体系关键技术

3.1　密钥监控与分析

针对不同业务系统应用模式差异大,管理单一分散,管理和应用成本较高的特点,以对称密钥管理、非对称密钥管理、加密算法管理、密钥选型管理的密钥管

理模块为基础,构建密钥监控与分析系统,如图 3 所示。

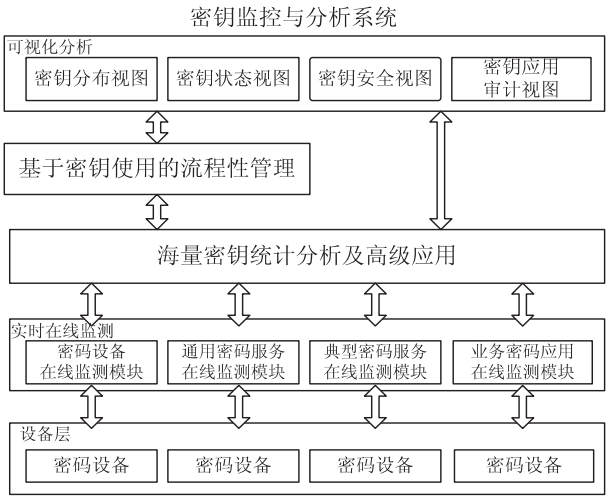

图 3 密钥监控与分析系统结构图

该系统主要实现如下功能:

1)实现基于事件统计、密钥统计、设备统计、用户统计和日志统计的密钥使用安全趋势分析预测;

2)通过海量、不同类型的密钥在密码设备上的检索预处理技术、快速检索技术,实现系统对密钥的快速检索;

3)通过高并发下大量密钥的存储技术、临时内存转储、延迟存储技术等技术,保证系统在高并发下的密钥安全可靠存储[14];

4)针对密码设备、密码服务、密码使用者,根据密钥使用及管理的安全需求制定密钥合规性、有效性监测策略和判定策略,并基于该策略实现对密钥合规性、有效性、安全性的实时监测;

5)通过对监测指标数据的统计、挖掘,对结果进行定性或定量分析,实时展现各类密钥在各业务的分布视图、状态视图(包括密钥生成事件、更新事件等)、安全视图(包括密钥有效期、合规性告警),及用户操作审计等信息,实现基于事件统计、密钥统计、设备统计、用户统计和日志统计的密钥使用安全趋势分析预测。

3.2 密钥安全性检测

在整个统一密钥支撑体系中,密钥安全性检测平台主要对信息技术产品/系统、网络密码和安全协议为业务对象的商品密码安全性进行检测评估,建立密钥合规性及合法性安全评价流程,针对企业应用系统的实际情况,更规范、更合法地使用密码技术,保障基础网络和重要信息系统的安全性。

密钥安全性检测如图 4 所示。

3.2.1 系统密钥使用分级

建立系统密钥使用分级机制。依据系统的密钥规模、系统的重要程度、系统所属的级别进行评级,根据不同的分级分别作不同的安全要求,将有利于系统的安全管理和顺利运行。分级管理将有效地提高系统安全要求和资源方面的投入。

密钥安全性检测		
系统密钥使用分级 · 密钥规模 · 系统特点 · 部署级别	密钥安全评测 · 密码算法 · 密钥强度 · 密钥合规性 · 密钥合法性	产品评测 · 资质审查 · 产品功能 · 产品性能 · 环境参数

图 4 密钥安全性检测

3.2.2 密钥安全评测

在构建密钥安全评测能力过程中将会用到多种评测技术,常用的有随机数检测、密码协议形式化分析、算法正确性检测技术等。

1) 随机数检测:随机数在密码应用中发挥着极其重要的作用,例如密码算法里的密钥要求是随机数,另外许多密码协议的中间过程也需要随机数,随机数的安全性将会直接影响到所有对称密钥、非对称密钥的安全性,甚至是整个系统的安全性。随机数的检测方法有单比特频数检测、块内频数检测、扑克检测、重叠子序列检测、游程总数检测、游程分布检测、块内最大“1”游程检测、二元推导检测、自相关检测、矩阵秩检测、累加和检测、近似熵检测、线性复杂度检测、Maurer 通用统计检测、离散傅里叶检测等技术[15]。

2) 密码协议形式化分析:密码协议的设计是困难且易于出错的,有些密码协议往往不如他们的设计者所期望的那样安全,所以密码协议的执行具有高度不确定性,即便是对有限条件约束下的密码协议也要求分析潜在无限可能的攻击者行为。形式化分析方法是检测密码协议是否安全的一种重要技术,通过该技术可以检测密码协议是否存在缺陷和安全漏洞。针对企业业务系统对称、非对称密钥及数字证书的实际应用模式及各分析方法的特点,采用 Hoare 逻辑分析方法对业务系统的安全通信协议及密码应用算法进行形式化分析,使得检测平台可高效地分析出系统可能存在的安全漏洞、密钥应用的不合规性,进一步提高系统整体的安全性及可靠性。

3) 算法正确性检测:密码算法是密码应用系统的核心安全内容,选择符合国家管理规定的密码算法是保证系统的首要条件,但是密码算法的实现或使用过程中如果没有严格按照要求,可能会导致应用系统的输入输出数据不符合标准,无法与其他的系统或模块进行正确的通信和交互。算法正确性检测主要保证密码软件中程序的执行符合相应的设计规范,保证程序执行的输入、输出行为和设计规范相匹配。在算法正确性检测前,应该先建立评测样本,其中包含各种标准

密码算法的输入输出数据。

3.2.3　产品评测

开展密码产品评测。评测应用系统所使用的密码算法是否是符合国家密码管理局批准使用的算法,密码设备和密钥的使用过程是否符合国家法律法规要求,所使用的密码设备或密码软件是否具有相关的产品资质,是否符合其标称的规格参数,是否满足应用要求,如功能参数、性能参数、环境参数等。

4　结束语

该研究构建了以密钥管理体系及标准,密钥监控与分析系统和密钥安全性检测平台为基础的统一密钥支撑体系,通过试点建设,成功地解决了企业密钥使用中存在的实际问题与需求,为业务系统的密钥应用提供有效的服务与支撑,为移动化和互动化终端提供适用的密钥选型与灵活的密码服务机制,提高密钥管理能力及效率,提升密钥安全应用水平,增强业务应用安全防护能力,可在国家重要行业和大型企业的信息安全防护工作起到引领和示范效果。

参考文献:

[1] Steve G A. 公开密钥基础设施-概念、标准和实施[M]. 冯登国,译. 北京:人民邮电出版社,2001.

[2] Mao Wenbo. 现代密码学理论与实践[M]. 王继林,伍前红,译. 北京:电子工业出版社,2006.

[3] 艾　俊,吴秋新. 可信计算密码支撑平台中的密钥管理技术研究[J]. 北京信息科技大学学报,2009,24(4):92-96.

[4] 杨　波. 可信计算平台密钥管理机制的应用与研究[D]. 西安:西安电子科技大学,2008.

[5] 全国信息安全标准化技术委员会. GB/T 20518-2006 信息安全技术公钥基础设施数字证书格式[S]. 2006.

[6] 全国信息安全标准化技术委员会. GB/T 20520-2006 信息安全技术公钥基础设施特定权限管理中心技术规范[S]. 2006.

[7] 许丽京. 可信计算技术安全协议与密钥管理研究[J]. 数据通信,2007(2):41-45.

[8] 张　淼,杨　昌,孙　琪,等. 可信计算平台中的密钥管理[J]. 楚雄师范学院学报,2006,21(9):17-22.

[9] 同鸿滨. 密钥托管系统的研究与设计[D]. 成都:四川师范大学,2006.

[10] 庄　湧. PKI 中的可验证部分密钥托管[J]. 计算机学报,2006,29(9):1584-1589.

[11] 谢颖莹. 基于 PKI 的身份认证系统的研究与实现[D]. 北京:华北电力大学,2006.

[12] 刘知贵,杨立春,蒲　洁,等. 基于 PKI 技术的数字签名身份认证系统[J]. 计算机应用研究,2004,21(9):158-160.

[13] 史创明,王立新. 数字签名及 PKI 技术原理与应用[J]. 微计算机信息,2005,21(8):122-124.

[14] 魏家好,侯整风. 基于(n,r)门限的密钥恢复方案[J]. 计算机技术与发展,2006,16(10):134-136.

[15] 王平水. 公钥密码体制及其安全性分析研究[D]. 合肥:合肥工业大学,2006.

(上接第 112 页)

参考文献:

[1] Gallagher M, Narasimhan V L. ADTEST: A test data generation suite for Ada software systems[J]. IEEE transactions on software engineering, 1997, 23(8): 473-484.

[2] 刘　磊,邹黎敏,胡兴凯,等. 基于模块化的软件可靠性模型[J]. 西南师范大学学报(自然科学版),2010,35(2):100-102.

[3] 谈维新,沈元隆. 考虑测试效率的软件可靠性模型研究[J]. 计算机技术与发展,2011,21(8):67-70.

[4] 张　玲,袁　娜,马永刚,等. 基于测试用例和时间域软件可靠性模型[J]. 计算机技术与发展,2009,19(11):167-170.

[5] Lyu M F. Handbook of software reliability engineering[M]. USA: McGraw-Hill Companies, 1996.

[6] 黄锡滋. 软件可靠性,安全性与质量保证[M]. 北京:电子工业出版社,2002.

[7] 刘　丹. 软件测试及可靠性研究[D]. 长春:长春理工大学,2009.

[8] 腾灵灵,邵　栋,荣国平. 软件可靠性模型选择研究[J]. 计算机应用与软件,2010,27(6):128-131.

[9] Musa J D. 软件可靠性工程[M]. 北京:机械工业出版社,2003.

[10] Sommerville L. Software engineering[M]. 8th ed. Beijing: China Machine Press, 2007.

[11] 魏传程. 软件可靠性建模及最优化问题研究[D]. 燕山:燕山大学,2010.

[12] 苗　扬. 软件可靠性测试与评估方法的改进[D]. 上海:上海交通大学,2009.

统一密钥支撑体系的研究

作者： 刘金锁， 黄益彬， 杨维永， LIU Jin-suo， HUANG Yi-bin， YANG Wei-yong
作者单位： 国网电力科学研究院,江苏 南京,210006

刊名： 计算机技术与发展

ISTIC

英文刊名： Computer Technology and Development

年，卷(期)： 2014(3)