PSTunnel-2000

电力系统专用

纵向加密认证网关

技术白皮书（v2.0）

中国电力科学研究院

北京科东电力控制系统有限责任公司

2007 年 7 月

目录

1 公司简介

1.1 中国电力科学研究院

•中国电力建立最早、专业最齐全的研究院，迄今已有 50 年历史；

•有科学院院士、工程院院士及许多电力系统著名专家；

•有研究生部、博士点及博士后流动站；

•形成许多品牌产品：如 CC-2000 调度自动化系统在中国网、省调度自动化系统占有率居全国第一，并荣获 2000 年国家科技进步一等奖；

•通过 ISO 9001（2000 版）的质量认证。

1.2 科东公司

北京科东电力控制系统有限责任公司(电网所)隶属于中国电力科学研究院，是一个专门从事电力系统自动化方面的技术开发、技术服务、技术咨询、技术培训及工程承包等工作的高新技术软件企业。注册资金 1000 万元。

1.2.1 技术力量

科东公司现有中高级以上职称技术人员 180 多人，其中既有作为博士、硕士研究生导师的著名老专家学者，也有博士硕士并具有丰富实践经验的中青年专家。

从成立至今，科东公司已完成大小共几十项电网调度自动化系统工程。

电网所与国家电力公司科技环保部、调度通信中心一起完成了电力调度专用数据网络及电力二次系统安全防护的规划，并成功地申请了国家 863 计划；

电网所是国家电力二次系统安全防护专家组成员（王文博士、杨秋恒教授、高昆仑博士），制定了《全国电力二次系统安全防护的总体方案》；

电网所是国家电力二次系统安全防护工作组成员（王文博士、杨秋恒教授、高昆仑博士），对各地网省调度中心的二次系统安全防护方案进行评审，对各地网省调度中心的二次系统安全防护的实施情况进行了检查。

1.2.2 组织结构

科东公司实行董事会领导下的总经理负责制。由总经理、副总经理全面负责公司运营、技术工作，下设电网调度自动化、配电自动化、应用仿真、电力市场、技术开发、市场、销售、人事行政、质量管理、东北分公司、南方分公司等部门开展各项业务。

1.2.3 为您提供的服务

在电力二次系统安全防护领域竭诚为您提供以下服务：

电力二次系统网络安全防护方案的设计与实施；

电力专用网络安全设备系列产品，包括正向型、反向型隔离设备、纵向加密认证装置、安全网关机、调度证书系统。

关于电力二次系统安全防护的咨询和培训。

2 装置的开发背景

中国电力科学研究院（电网所）/北京科东电力控制系统有限责任公司作为国家电力调度通信中心主持的《全国电力二次系统安全防护方案》研究课题的参与单位，派出了多名工作人员参与电力二次系统安全防护专家组工作，从事总体方案、技术方案、实施方案的编写，并受国家电力调度通信中心委托开发电力系统专用网络安全产品。

按照全国电力二次系统安全防护的要求，该电力专用网关的研制是国家电力公司科技环保部 2000 年科技攻关项目，是国家 863 项目—国家电网调度中心二次系统安全防护的子课题。

3 开发的依据和功能规范

- 国家电网调度中心发布《全国电力二次系统安全防护方案（最新版）》
- 国家电网调度中心制定《电力系统专用纵向加密认证装置技术规范（最新版）》
- 中华人民共和国国家标准 GB/T 17900-1999《网络代理服务器的安全技术要求》
- 《关于维护网络安全和信息安全的决议》，全国人大常委会 2000 年 10 月审议通过；
- 《中华人民共和国计算机信息系统安全保护条例》，国务院 1994 年发布；
- 《涉及国家秘密的通信、办公自动化和计算机信息系统审批暂行办法》，

国家保密局 1998 年发布；

- 《计算机信息网络国际联网安全保护管理办法》，公安部 1998 年发布；
- 《计算机信息系统安全保护等级划分准则》(GB 17859-1999)，公安部 1999 年发布；
- 《电网和电厂计算机监控系统及调度数据网络安全防护规定》，国家经贸委[2002]第 30 号令；
- 《电力工业中涉及的国家秘密及具体范围的规定》，电力工业部和国家保密局 1996 年发布。
- GB/T 14598.9-1995　辐射电磁场抗扰度标准
- GB/T 14598.10-1996　快速瞬变抗扰度标准
- GB/T 14598.13-1998　脉冲群抗扰度标准
- GB/T 14598.14-1998　静电放电抗扰度标准
- GB/T 17626.5-1999　浪涌（冲击）抗扰度标准
- GB/T 17626.6-1998　射频场感应的传导骚扰抗扰度标准
- GB/T 11287-2000　机械振动响应标准

4 参考的安全标准和规范

UL 1950

EN 41003

AS/NZS 3260

AS/NZS 3548 Class A

CSA Class A

FCC Class A

EN 60552-2

VCCI(ClassII)

5 我方涉密资质证明和涉密立项

我方已经向国家密码管理委员会申请作为“国家密码产品定点生产单位”和“国家密码产品定点销售单位”，已经接受了国家密码管理委员会和北京市国家密码管理委员会的审查。

装置采用涉密芯片审批和批复

该装置采用电力系统专用算法密码芯片，并且已经通过国家密码管理委员会办公室批准立项，项目名为“SJY99 加密网关”，项目批文号为：国密办字[2004]292 号。

加密算法

纵向加密认证装置使用的密码算法包括对称加密算法、非对称算法、散列算法和随机数生成算法， 其中的对称算法是经过国密办批复的专为电力系统使用的加密算法。其他算法都是国密办指定的算法。

6 PSTunnel2000 电力专用加密认证网关

6.1 型号

PS—Tunnel2000 电力专用纵向加密认证网关

6.2 系统组成

硬件平台

- 采用非 Intel 指令集的处理器， PowerPC 平台 PowerPC8245 400MZ；
- 内存〉=64M；
- 该网关采用已经集成在标准 PCI 卡上的采用国家密码办审批的电力系统专用的“SSX06 型密码算法芯片”的 PCI 加密卡作为网络报文加密解密、证书签名验签的“安全模块”；
- 该网关加密卡采用双密码算法芯片。

操作系统

代码可控的经过裁减内核的 Linux 作为操作系统。

配置软件

- 纵向加密认证网关提供了良好的用户接口和管理界面。方便简易的配置界面，可以使该装置的配置简单易行。配置信息包括对装置的设备基本信息的配置、高可用信息、双机热备功能的配置，日志功能的定制和配置，该装置的工作模式的配置。

6.3 内部硬件模块

- 采用双电源交流 110V-220V、直流 100V-370V 供电， 保证系统供电模块的可靠性；
- 具有五个不同功能接口 10/100/1000M 自适应网口的网卡， 保证网络传输的高速稳定；

- 支持双网通信；
- 旁路网口作为紧急应急接口， 当通信设备故障时，设备断电，设备自动启动旁路功能，此时设备恢复明文通讯。
- 物理锁具。 保证加密装置内部安全模块的安全，没有特定的钥匙， 不能打开机箱外壳，不能看见“加密认证网关”密码装置内部的结构和安全密码卡的结构。保证“加密认证网关”密码装置的物理安全。
- 采用国家电力调度通信中心指定的 IC 卡生产厂家的 IC 卡，作为该装置的管理人员的“人机卡三方认证”的登录安全介质。
- 该网关外形为 1U 标准的机箱：重量为 4kg，上架方式为面板前方左右两侧的钢质耳朵。
- 有蜂鸣器装置作为声音报警装置， 一旦系统发生紧急情况，可以由该系统的报警模块出发，作为提示系统管理人员的声音警示。
- 在装置的前方配有液晶显示屏，作为系统状态显示的外部接口， 可以动态显示系统内部硬件和软件运行状态的不同的状态信息， 方便用户了解系统运行的状态， 及时发现可能遇到的各种问题，减少系统故障带给电力控制系统运行造成的损失。
- 面板前后方分别有多个指示灯， 分别代表系统电源状态，内置读卡器状态，IC 卡状态，不同网口状态，外接的系统信息串口状态，报警模块外部接口的状态，内部处理模块状态， 安全加密解密模块等系统关键部件的运行状态。
- 内置硬件 Wacthdog， 用以监视系统的运行状态，保证整个硬件电路的安全稳定、可靠。
- 内置 RTC 时钟模块， 保证系统时间的精准。

6.4 接口规范

- RJ45 转 RS232 CONSOLE 的接口；
- 4 个 1000M 网口，2 个 100M 网口，两个光口与其中的两个千兆网口复用， 一个配置网口，一个扩展网口；
- 两个交流 110V-220V、直流 100V-370V 电源插座；
- 两个电源开关；
- IC 卡接口，符合 ISO－7816 智能 IC 卡规范。

6.5 电气性能

- 电源

  交流 110V-220V、直流 100V-370V

- 环境规范

  运行温度：-5℃ -- +45℃（-15℃贮藏运输）

  操作湿度：10% -- 90%@40 摄氏度，非冷凝

- 大气压力：

  70kPa～106kPa

6.6 几何及物理特性

- 尺寸：标准 1U 机箱
- 重量：4kg

6.7 抗干扰性

- 辐射电磁场抗扰度 :能承受 GB/T15153.1 中规定的严酷等级为 3 级（6V/m）的辐射电磁场干扰实验，性能符合 GB/T17626.1 总则 9 中 “a)” 规定的要求。
- 快速瞬变抗扰度:电源和信号都能承受 GB/T15153.1 中规定的严酷等级为 3 级的快速瞬变干扰实验，性能符合 GB/T17626.1 总则 9 中 “a)” 规定的要求。
- 脉冲群抗扰度装置: 能承受 GB/T15153.1 中规定的严酷等级为 3 级的 1MHz 和 100kHz 的脉冲群干扰实验，性能符合 GB/T17626.1 总则 9 中 “a)” 规定的要求。
- 静电放电抗扰度: 能承受 GB/T15153.1 中规定的严酷等级为 3 级的静电放电干扰实验，性能符合 GB/T17626.1 总则 9 中 “a)” 规定的要求。
- 浪涌（冲击）抗扰度: 能承受 GB/T15153.1 中规定的严酷等级为 3 级的浪涌（冲击）干扰实验，符合 GB/T17626.1 总则 9 中 “a)” 规定的要求.
- 机械振动装置: 能承受 GB/T11287－2000 中 3.2 中规定的严酷等级为 1 级振动实验，性能符合该标准 5 中规定的要求。
- 工频磁场装置: 能承受 GB/T15153.1 中规定的严酷等级为 4 级的工频磁场干扰实验，性能符合 GB/T17626.1 总则 9 中 “a)” 规定的要求。
- 介质强度装置: 能承受 GB/T15153.1 中规定的严酷等级为 3 级的绝缘强度(不小于 5MΩ ）和耐压强度（电源输入回路不小于 1500V ）实验，性能符合 GB/T17626.1 总则 9 中 “a)” 规定的要求。
- 稳定性装置: 能承受 GB/T13729 中 3.9 规定的稳定性实验;
- 其他参考标准

  IEC-1000-4-2 （ESD）

IEC-1000-4-3 （辐射敏感性）

IEC-1000-4-4 （电快速瞬变）

IEC-1000-4-5 （电涌）

IEC-1000-4-6 （谐波）

6.8 基本功能

- 纵向加密认证装置中使用的非对称密码功能部分，是基于证书的公私钥验证体系，与现在已经投入运行的各个网省电力调度中心的“电力调度证书服务系统”相配合。证书的格式完全符合 X509 证书规范，与“电力调度证书服务系统”各个厂家所签发的证书完全兼容；
- 专有加密通信协议：加密认证网关间通信协议为国调组织多位专家联合设计，并经权威机构的多位院士审查论证，通信协议内容同样高度保密；
- 在纵向加密认证装置通信加密协议包括会话密钥协商和通信加密两个阶段。第一阶段的密钥协商需要完成纵向加密认证装置之间的认证和用于通信加密的会话密钥协商。第二阶段完成加密数据的通信；
- 电力专用纵向加密认证网关能够实现“电力二次系统安全防护总体方案”中要求的安全防护功能，满足二次系统安全防护要求；
- 我方提供的“纵向加密认证网关”在和不同厂家之间的纵向加密认证网关、装置已经能保证互连互通；
- 纵向加密认证网关能被其对应的管理中心管理， 具备可管理性；
- 已经通过电力系统指定单位的电磁兼容性检测；
- 支持双机热备功能，在任一设备出现故障时，自动切换；

- 采用代码可控的安全操作系统， 经过裁剪内核网络功能的 Linux 操作系统；
- 本身应能够一定程度防御常见的网络攻击，包括 ARP Attack、Ping Attack、Ping of Death Attack、Smurf Attack、Unreachable Host Attack、Land Attack、Teardrop Attack、Syn Attack 等；
- 在对纵向加密认证网关进行管理时，需要“人机卡”的三方认证过程。管理人员必须持有可用于管理的智能 IC 卡， 必须持有可登陆管理的密码，再进行过“人机卡”的三方认证才能登陆纵向加密认证网关模块， 进行有效的管理配置。

6.9 产品特点

- 作为对电力专用的加密认证网关，很好的结合了对电力系统内专用协议的兼容性，支持"IEC-104"，"DL476-92"的协议，可以很好的对以上协议进行解析和保护；
- 在纵向加密认证网关的工作模式支持多种模式， 充分考虑了该装置在部署过程中的不同网络情况的要求。在透明状态下工作时候，可以完全透明的接入该装置，不用对原来网络的结构有任何改变； 在网关工作模式下， 可以代理网关机应答；
- 纵向加密认证网关在工作时 ， 支持报文的抗重播功能， 有效的禁止报文重放；
- 纵向加密认证网关提供了良好的监视功能， 能对设备的状态信息、隧道的信息、基于隧道之上的安全策略信息进行监视；
- 方便的和管理中心进行连接和信息反馈，多次和管理中心的研制单位“国家

电网公司信息安全实验室”进行联调，完全支持该管理中心的查询和配置。快速的信息反馈有力的支持了管理中心的可管理性；

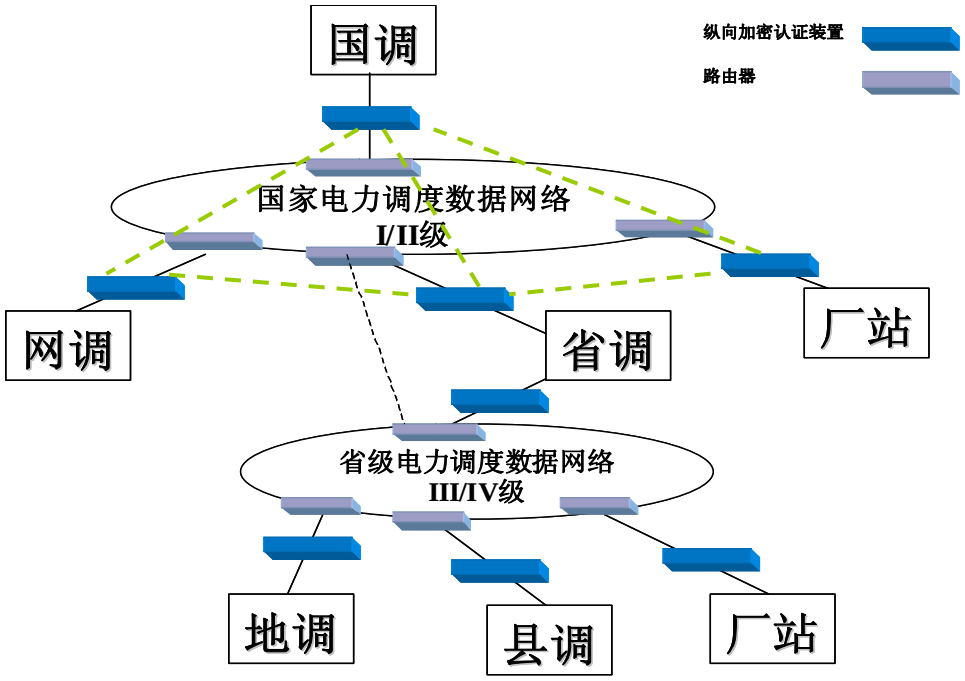
- 良好的在线帮助， 有效的支持用户的可操作性和对装置操作步骤的完整性；
- 高可用功能。按照功能规范要求，我方已经实现了纵向加密认证装置的双机热备和主备自动切换功能， 在切换过程中，安全隧道重新进行协商，快速的进行认证和加密传输处理工作，保障通信连续性。通过装置及其相关网络设备的冗余，增强网络接入环节的可靠性。从所保护的子网中的通信机到本地接入路由器之间的路径上，任何环节，包括设备或链路出现故障，加密装置都能正确识别，配合实现路径切换；
- 纵向加密认证装置对进行的操作和发生的事件均有日志记录，格式完全按照“SYSLOG”规范。 日志信息包括时间、事件类型，记录内容。该日志内容可以分别通过不同用户的需求和配置， 通过“串口”或者“网口”进行日志信息的发布和相应报警信息的引出。可以导出日志信息， 备份到本地硬盘中；
- 提供查看内部证书信息的命令， 将已经导入的远程证书信息、本地设备证书、操作员证书、管理中心证书等证书信息；
- 提供本地进程监视和终止的功能。可以在本地管理的图形界面中，查看本机内部的进程状态信息。只要输入友好终止的进程号， 就可以终止本地的某个进程；
- 对于初始化状态和装置的正常运行状态的转换。管理软件可以简洁的通过“初始化向导”配置将设备的初始化状态转入“正常运行状态”；
- “电力纵向加密认证网关/装置”有特殊探测报文，类似 PING 功能， 能够

显示出来对方装置的 安全模式是安全还是旁路，设备状态是正常还是异常，设备是主还是备；

- 支持管理中心发出的监视和管理报文。支持路由器 trunk 协议。根据设备接入口的需要， 需要 VLAN ID 的配置和驱动支持.同时支持 802.1Q 的标准和思科标准两种不同的二层以太网报文的解析和转发。

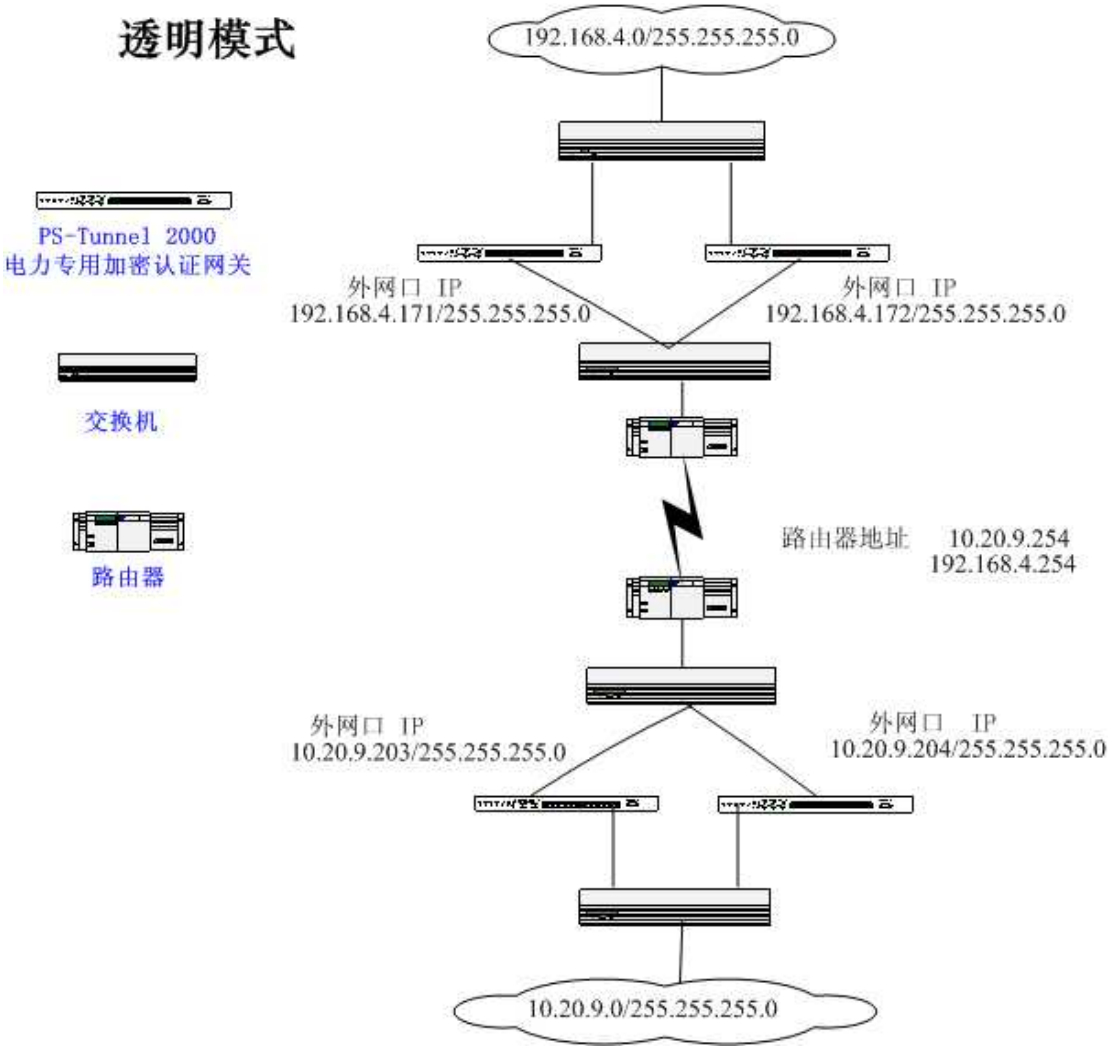
6.10 部署位置以及和管理中心的关系

按照“分级管理”要求，纵向加密认证装置部署在各级调度中心及下属的各厂站，根据电力调度通信关系建立加密隧道（原则上只在上下级之间建立加密隧道），加密隧道拓扑结构是部分网状结构。如图：



各个纵向加密认证网关 之间部署示意图

典型网络配置


透明模式
192.168.4.0/255.255.255.0
PS-Tunnel 2000
电力专用加密认证网关
外网口 IP
192.168.4.171/255.255.255.0
外网口 IP
192.168.4.172/255.255.255.0
交换机
路由器
路由器地址 10.20.9.254
192.168.4.254
外网口 IP
10.20.9.203/255.255.255.0
外网口 IP
10.20.9.204/255.255.255.0
10.20.9.0/255.255.255.0

附录：相关其他系统简介

电力调度证书服务系统

国家电力调度通信中心和网省级 30 余个调度中心，已经于 2005 年 4 月投入运行了电力调度证书服务系统。

我方开发研制“PS—Cert2000 电力调度证书服务系统”。

目前我方的“PS—Cert2000 电力调度证书服务系统”已经在国调、华北、东北、华中网调和 10 余个省级电力调度中心正常运行。

其中， 国调的根证书系统是我方的“PS—Cert2000 电力调度证书服务系统”， 其余网省的证书服务系统是中级证书服务系统， 可以为下级地调中心签发证书系统和该级系统各个应用和用户签发证书。

电力专用纵向加密认证装置/网关管理中心：

由国家电网公司信息安全实验室（中国电力科学研究院通信所）负责开发研制的，专门为管理“ 电力专用纵向加密认证网关/设备”的专用网络设备管理中心。一般部署在调度通信中心。

负责监视和管理纵向加密认证装置或者网关。