(19)中华人民共和国国家知识产权局

(12)发明专利

(10)授权公告号 CN 104184735 B
(45)授权公告日 2018.03.09

(21)申请号 201410423475.1

(22)申请日 2014.08.26

(65)同一申请的已公布的文献号
申请公布号 CN 104184735 A

(43)申请公布日 2014.12.03

(73)专利权人 国网浙江省电力有限公司
地址 310007 浙江省杭州市西湖区黄龙路8号
专利权人 国网浙江省电力公司嘉兴供电公司
国家电网公司

(72)发明人 涂莹 肖世杰 张燕 裘华东 叶盛 郑斌 胡若云 丁麒 沈然 金良峰 颜拥 黄瑞章 刘欢 李南 马闯 沈超 孙一申 和巍 糜晓波 畅伟 吕诗宁 谷泓杰 林恺丰 吴慧

(74)专利代理机构 浙江翔隆专利事务所(普通合伙) 33206
代理人 戴晓翔 王晓燕

(51)Int.Cl.
H04L 29/06(2006.01)
H04L 9/00(2006.01)
G06Q 50/06(2012.01)
G06Q 30/02(2012.01)

(56)对比文件
CN 103441991 A,2013.12.11,
US 2013013669 A1,2013.01.10,
CN 202652534 U,2013.01.02,
凌行龙等.电力营销移动作业安全分析及防护研究.《ELECTRIC POWER ICT》.2013,
郭宝等.电力生产现场作业和终端安全防护研究.《深信服科技》.2010,正文第1-5节,图7.
赵永彬等.电力企业移动办公系统的研究与设计.《辽宁电力信息化建设成果专栏》.2011,全文.
秦超等.基于数字证书认证的电力移动作业安全接入系统.《中国电机工程学会电力通信专委会第八届学术会议论文集》.2011,
秦超等.电力移动作业PDA安全接入系统设计与实现.《电力系统自动化》.2012,

审查员 李星星

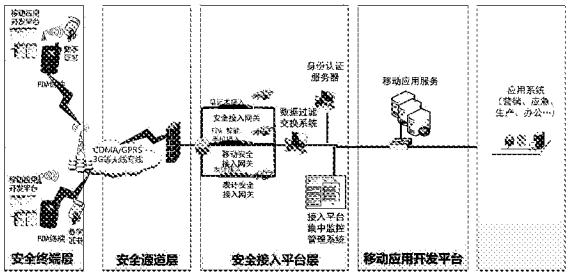
权利要求书3页 说明书6页 附图1页

(54)发明名称

电力营销移动应用安全防护系统

(57)摘要

电力营销移动应用安全防护系统,涉及一种电力营销移动应用系统。目前,采用移动终端后将产生安全问题,采用第三方的二次加密,容易破解,产生信息的泄露。本发明包括:安全终端层;安全通道层;安全接入平台层;移动应用层:用于支持移动终端的业务应用,实现系统的应用安全。本技术方案实现了移动终端的安全接入,通过隔离手段实现信息内网、信息外网的强隔离,切断外网的攻击,有效地提升了信息安全。



CN 104184735 B

1.电力营销移动应用安全防护系统，其特征在于包括：

安全终端层：移动终端使用加密算法，并在移动终端上保存私钥或者数字证书；移动终端通讯时通过移动公网与安全接入网关群建立安全通道，采用数字证书进行身份认证，并对通讯关键数据进行加密传输；

安全通道层：实现各个外部链接与系统接入网连接，通过路由访问控制，并通过VPN构建的加密虚拟专用通道，实现网络级身份认证，并保证数据机密性和完整性；通过防火墙进行边界区的访问控制，防止非法设备的接入应用；配置相应的安全监测系统，对接入应用安全隐患进行监测、防护和管理，确保安全接入与系统接入网部分的安全；对接入网与企业内网之间从物理层到应用层所有层次的通信协议进行隔离，为每一个允许的应用建立和维护一个专用数据交换机制，限定数据交换的源、目的、数据格式、数据内容，并对数据交换进行监控；

安全接入平台层：为对外信息发布、信息采集、数据交换的中间区域，是接入终端网络连接的终点，所有应用访问终止于安全认证网关；安全接入平台层对交换业务注册、运行情况进行安全检测与审计，对网络设备、安全设备的配置管理及日常运行进行维护，对安全策略管理、流量监测、统计分析、安全审计以友好及人性化界面进行展示；

移动应用层：用于支持移动终端的业务应用，实现系统的应用安全；

营销移动应用安全防护层次为：

企业内网通过数据加密实现应用数据安全，通过审计/授权和安全隔离实现应用系统安全；

客户端安全接入系统通过KEY认证/引导和桌面控制系统实现操作系统安全；通过VPN安全接入和数字证书认证实现接入安全；通过商密算法加密和二次认证实现物理网络安全；

营销移动应用安全防护层次内容包括：

1)安全接入是整个平台的核心，第三方网络与企业信息网络之间构建安全接入区，进行网络的安全分隔；通过平台的安全接入、认证、访控服务进行安全接入；

2)通过建立不依赖于第三方运营商的二次加密隧道，增强数据传输安全性，经过安全接入区，进行用户身份的认证、数据加密、用户数据的审计/授权、文件的在线加密；

3)VPN网关接入服务层是核心部分，包括安全接入网关系统、身份认证系统、数据加解密、集中监控管理用户逻辑功能组件，功能组件之间通过高速消息总线进行通信，实现各种安全服务；

4)根据用户需求差异、应用差异、网络改造需求，安全接入平台系统功能组件、数据安全保护系统功能组件，按照接入平台思想进行分段式组合部署，并进行网络层的无缝对接；

5)身份认证系统，终端与VPN实行双向认证，并且通过CA服务认证授权；数字证书保障登陆安全平台系统的用户，都是通过管理认证的用户；数字证书的发放、撤销、过期重申请，既能以通过OCSP协议在线方式，又能以通过离线的方式，由专人手动管理；

6)防火墙，安全平台的接入边界，这是用户进入安全平台的首个对数据的安全过滤；防火墙是一种综合性的技术，涉及到计算机网络技术、密码技术、安全技术、软件技术、安全协议多方面；是一种网络安全的保障手段；是网络通信时执行的一种访问控制尺度，其目标包括通过控制入、出一个网络的权限，并迫使所有的链接都经过这样的检查；

所有的外部用户数据到内部的企业内网的业务流均要经过防火墙，利用防火墙的网络地址翻译的功能和数据的安全过滤，对需要保护的网络进行保护；

7)安全接入网关

IPSEC VPN接入网关，为用户远程访问网络服务提供安全保护，功能包括：

身份认证：配合数字证书体系，确保远程访问者不是恶意用户；

访问控制：确保访问者只能访问被授权访问的服务和信息；

数据加密：配合SDKey中提供的商密算法，确保所有数据在网络传输过程中都是被加密的，防止被破解；

SSL VPN接入网关，为用户远程访问网络服务提供安全保护，功能包括：

身份认证：配合数字证书体系，确保远程访问者不是恶意用户；

访问控制：确保访问者只能访问被授权访问的服务和信息；

数据加密：配合SDKey中提供的商密算法，确保所有数据在网络传输过程中都是被加密的，防止被破解；

8)安全隔离系统

安全隔离与信息交换系统，俗称“网闸”，网络隔离技术的目标是确保把有害的攻击隔离，在可信网络之外和保证可信网络内部信息不外泄的前提下，完成网间数据的安全交换；网络隔离技术是在原有安全技术的基础上发展起来的，弥补了原有安全技术的不足，突出了自己的优势，是安全子网与企业内网的安全隔离系统，保障访问业务内网的安全；

9)审计、授权系统

安全审计系统通过网络数据的采集、分析、识别，实时动态监测通信内容、网络行为和网络流量，发现和捕获各种敏感信息、违规行为，实时报警响应，全面记录网络系统中的各种会话和事件，实现对网络信息的智能关联分析、评估及安全事件的准确全程跟踪定位，为整体网络安全策略的制定提供权威可靠的支持。

2.根据权利要求1所述的电力营销移动应用安全防护系统，其特征在于：所述的安全接入平台层设有接入网关、数据过滤交换系统、身份认证服务器及接入平台集中监控管理系统，所述的接入网关包括用于笔记本接入的安全接入网关、用于PDA/智能手机接入的移动安全接入网关、用于表计接入的表计安全接入网关。

3.根据权利要求2所述的电力营销移动应用安全防护系统，其特征在于：当智能终端为平板电脑、PDA或智能手机时，安全终端层使用的安全算法私钥或者数字证书采用MicroSD卡进行存储；在智能终端上设SIM卡，通过绑定专用APN的SIM卡实现网络通道安全；并在智能终端部署安全专控软件，实现安全通道建立、用户认证管理。

4.根据权利要求3所述的电力营销移动应用安全防护系统，其特征在于：移动应用层设移动应用服务器，应用服务器部署防病毒模块，保证应用服务区各应用服务器不被病毒、木马感染，防止病毒的传播和非法控制。

5.根据权利要求1所述的电力营销移动应用安全防护系统，其特征在于：所述的安全通道层、安全接入平台层、移动应用开发平台组成移动作业平台，所述的移动作业平台设有信息安全与防护单元、跨平台的业务支撑单元、应用支撑单元、移动GIS的支撑单元、移动工作流支撑单元、平台管理单元；所述的信息安全与防护单元用于安全接入平台VPN无线接入支撑、应用服务的报文加密通讯、移动终端的数据库安全加密以实现高效和安全接入；所述的

跨平台的业务支撑单元用于支持多种移动终端操作系统，通过支持多种操作系统，同时建立一套统一规范的API来适应各操作系统以实现跨平台的支持，并支持多种终端硬件；所述的应用支撑单元用于硬件底层支撑；所述的移动GIS的支撑单元用于地理图形展示、电网资源展示、GIS空间分析、路径导航、位置上报；所述的移动工作流支撑单元用于包括电力移动应用发布平台服务端和客户端的管理；所述的平台管理单元用于设备管理、权限管理、业务菜单管理、移动终端的状态监控、服务监控及标准化现场作业分析。

6.根据权利要求5所述的电力营销移动应用安全防护系统，其特征在于：应用支撑功能的硬件底层支撑单元用于：打印、位置服务、条码扫描、高射频卡读写、用户电子签名认证、移动终端网络状态通知、其他硬件特性封装；配备设备的审计登陆、用户登陆审计及服务组件的审计登陆认证；配备视频文件、图像文件、图案管理系统集成文件服务；任务数据发布、下载、导入审核；用户认证及安全策略管理。

7.根据权利要求1所述的电力营销移动应用安全防护系统，其特征在于：

安全接入平台层安全分隔第三方网络与企业信息网络，实现移动终端的安全接入；安全接入平台层进行用户身份的认证、数据加密、用户数据的审计/授权、文件的在线加密实现传输的安全性；安全接入平台层设有VPN网关接入服务层，VPN网关接入服务层包括安全接入网关系统功能组件、身份认证系统功能组件、数据加解密功能组件、集中监控管理用户逻辑功能组件，上述功能组件之间通过高速消息总线进行通信以实现各种安全服务。

8.根据权利要求7所述的电力营销移动应用安全防护系统，其特征在于：安全接入平台层进行分段式组合部署，并进行网络层的无缝对接；身份认证系统采用终端与VPN网关实行双向认证，并且通过CA服务认证授权。

9.根据权利要求8所述的电力营销移动应用安全防护系统，其特征在于：安全接入平台层进行审计/授权工作时，通过网络数据的采集、分析、识别，实时动态监测通信内容、网络行为和网络流量，发现和捕获各种敏感信息、违规行为，实时报警响应，全面记录网络系统中的各种会话和事件，实现对网络信息的智能关联分析、评估及安全事件的准确全程跟踪定位，为整体网络安全策略的制定提供权威可靠的支持。

10.根据权利要求9所述的电力营销移动应用安全防护系统，其特征在于：安全/审计工作包括：

内容审计

用于提供深入的内容审计功能，对网站访问、邮件收发、远程终端访问、数据库访问、数据传输、文件共享提供完整的内容检测、信息还原功能；并可自定义关键字库，进行细粒度的审计追踪；

行为审计

用于提供全面的网络行为审计功能，根据设定行为审计策略，对网站访问、邮件收发、数据库访问、远程终端访问、数据传输、文件共享、网络资源滥用的网络应用行为进行监测，对符合行为策略的事件实时告警并记录；

流量审计

用于提供基于协议识别的流量分析功能，实时统计出当前网络中的各种报文流量，进行综合流量分析，为流量管理策略的制定提供可靠支持。

电力营销移动应用安全防护系统

技术领域

[0001] 本发明涉及一种电力营销移动应用安全防护系统。

背景技术

[0002] 在电力行业信息化不断推进的过程中，信息系统已经成为电力企业公司员工日常工作的基础手段，在电力生产控制与公司经营管理中发挥了日益重要的作用。然而越来越多的不便却是传统信息系统难以解决的，传统的必须在电力公司局域网内才能使用的管理软件给现场交流和服务质量提升造成了极大制约。在电力营销信息化工作不断深化的过程中，营销业务管理的信息系统用户在移动应用方面提出了具体的要求，如何在客户现场及施工现场随时处理工作，外勤人员如何在办公室外完成各种信息管理工作，各种原来现场人工记录数据无法及时录入管理系统的问题如何以更加灵活、方便的方式予以解决，以上种种问题，都可以使用移动终端进行解决，提高信息系统的便利性和处理效率，同时满足安全性要求。

[0003] 但采用移动终端后将产生安全问题，采用第三方的二次加密，容易破解，产生信息的泄露。内网接入条件严格，同时制约电力营销移动应用的发展。如何利用智能移动终端，通过外网安全的访问电力营销业务，成为一个迫切需要解决的重要课题。

发明内容

[0004] 本发明要解决的技术问题和提出的技术任务是对现有技术方案进行完善与改进，提供电力营销移动应用安全防护系统，以达到外网安全访问电力营销系统的目的。为此，本发明采取以下技术方案。

[0005] 电力营销移动应用安全防护系统，其特征在于包括：

[0006] 安全终端层：移动终端使用加密算法，并在移动终端上保存私钥或者数字证书；移动终端通讯时通过移动公网与安全接入网关群建立安全通道，采用数字证书进行身份认证，并对通讯关键数据进行加密传输；

[0007] 安全通道层：实现各个外部链接与系统接入网连接，通过路由访问控制，并通过VPN构建的加密虚拟专用通道，实现网络级身份认证，并保证数据机密性和完整性；通过防火墙进行边界区的访问控制，防止非法设备的接入应用；配置相应的安全监测系统，对接入应用安全隐患进行监测、防护和管理，确保安全接入与系统接入网部分的安全；对接入网与企业内网之间从物理层到应用层所有层次的通信协议进行隔离，为每一个允许的应用建立和维护一个专用数据交换机制，限定数据交换的源、目的、数据格式、数据内容，并对数据交换进行监控；

[0008] 安全接入平台层：为对外信息发布、信息采集、数据交换的中间区域，是接入终端网络连接的终点，所有应用访问终止于安全认证网关；安全接入平台层对交换业务注册、运行情况进行安全检测与审计，对网络设备、安全设备的配置管理及日常运行维护，对安全策略管理、流量监测、统计分析、安全审计，并以友好及人性化界面进行展示；

[0009] 移动应用层：用于支持移动终端的业务应用，实现系统的应用安全。

[0010] 作为对上述技术方案的进一步完善和补充，本发明还包括以下附加技术特征。

[0011] 所述的安全接入平台层设有接入网关、数据过滤交换系统、身份认证服务器及接入平台集中监控管理系统，所述的接入网关包括用于笔记本接入的安全接入网关、用于PDA/智能手机接入的移动安全接入网关、用于表计接入的表计安全接入网关。

[0012] 当智能终端为平板电脑、PDA或智能手机时，安全终端层使用的安全算法私钥或者数字证书采用MicroSD卡进行存储；在智能终端上设SIM卡，通过绑定专用APN的SIM卡实现网络通道安全；并在智能终端部署安全专控软件，实现安全通道建立、用户认证管理。

[0013] 移动应用层设移动应用服务器，应用服务器部署防病毒模块，保证应用服务区各应用服务器不被病毒、木马感染，防止病毒的传播和非法控制。

[0014] 所述的安全通道层、安全接入平台层、移动应用开发平台组成移动作业平台，所述的移动作业平台设有信息安全与防护单元、跨平台的业务支撑单元、应用支撑单元、移动GIS的支撑单元、移动工作流支撑单元、平台管理单元；所述的信息安全与防护单元用于安全接入平台VPN无线接入支撑、应用服务的报文加密通讯、移动终端的数据库安全加密以实现高效和安全接入；所述的跨平台的业务支撑单元用于支持多种移动终端操作系统，通过支持多种操作系统，同时建立一套统一规范的API来适应各操作系统以实现跨平台的支持，并支持多种终端硬件；所述的应用支撑单元用于硬件底层支撑；所述的移动GIS的支撑单元用于地理图形展示、电网资源展示、GIS空间分析、路径导航、位置上报；所述的移动工作流支撑单元用于包括电力移动应用发布平台服务端和客户端的管理；所述的平台管理单元用于设备管理、权限管理、业务菜单管理、移动终端的状态监控、服务监控及标准化现场作业分析。

[0015] 应用支撑功能的硬件底层支撑单元用于：打印、位置服务、条码扫描、高射频卡读写、用户电子签名认证、移动终端网络状态通知、其他硬件特性封装；配备设备的审计登陆、用户登陆审计及服务组件的审计登陆认证；配备视频文件、图像文件、图案管理系统集成文件服务；任务数据发布、下载、导入审核；用户认证及安全策略管理。

[0016] 安全接入平台层安全分隔第三方网络与企业信息网络，实现移动终端的安全接入；安全接入平台层进行用户身份的认证、数据加密、用户数据的审计/授权、文件的在线加密实现传输的安全性；安全接入平台层设有VPN网关接入服务层，VPN网关接入服务层包括安全接入网关系统功能组件、身份认证系统功能组件、数据加解密功能组件、集中监控管理用户逻辑功能组件，上述功能组件之间通过高速消息总线进行通信以实现各种安全服务。

[0017] 安全接入平台层进行分段式组合部署，并进行网络层的无缝对接；身份认证系统采用终端与VPN网关实行双向认证，并且通过CA服务认证授权。

[0018] 安全接入平台层进行审计/授权工作时，通过网络数据的采集、分析、识别，实时动态监测通信内容、网络行为和网络流量，发现和捕获各种敏感信息、违规行为，实时报警响应，全面记录网络系统中的各种会话和事件，实现对网络信息的智能关联分析、评估及安全事件的准确全程跟踪定位，为整体网络安全策略的制定提供权威可靠的支持。

[0019] 安全/审计工作包括：

[0020] a)内容审计

[0021] 用于提供深入的内容审计功能，对网站访问、邮件收发、远程终端访问、数据库访

问、数据传输、文件共享等提供完整的内容检测、信息还原功能；并可自定义关键字库，进行细粒度的审计追踪；

[0022] b) 行为审计

[0023] 用于提供全面的网络行为审计功能，根据设定行为审计策略，对网站访问、邮件收发、数据库访问、远程终端访问、数据传输、文件共享、网络资源滥用的网络应用行为进行监测，对符合行为策略的事件实时告警并记录；

[0024] c)流量审计

[0025] 用于提供基于协议识别的流量分析功能，实时统计出当前网络中的各种报文流量，进行综合流量分析，为流量管理策略的制定提供可靠支持。

[0026] 有益效果：实现统一信息交互、集中配置管理、统一监控等，实现对各类终端接入的可信、可控。基于本发明，实现电力营销移动作业(例如现场业扩、现场抄表、现场客服等营销业务应用)，提高营销业务客户现场的服务能力和优质服务水平，将客户服务进行空间和时间的延伸，使营销服务向客户现场延伸，在客户感知上树立优质服务、效率服务的形象。本技术方案实现了移动终端的安全接入。通过隔离手段实现信息内网、信息外网的强隔离，切断外网的攻击，有效地提升了信息安全。

附图说明

[0027] 图1是本发明的安全防护结构图。

[0028] 图2是本发明的安全防护层次图。

具体实施方式

[0029] 以下结合说明书附图对本发明的技术方案做进一步的详细说明。

[0030] 如图1所示，电力营销移动应用安全防护系统包含安全终端层、安全通道层、安全接入平台层、移动应用开发平台、应用系统等。

[0031] 其中，

[0032] 安全终端层：移动终端使用加密算法，并在移动终端上保存私钥或者数字证书；移动终端通讯时通过移动公网与安全接入网关群建立安全通道，采用数字证书进行身份认证，并对通讯关键数据进行加密传输；

[0033] 安全通道层：实现各个外部链接与系统接入网连接，通过路由访问控制，并通过VPN构建的加密虚拟专用通道，实现网络级身份认证，并保证数据机密性和完整性；通过防火墙进行边界区的访问控制，防止非法设备的接入应用；配置相应的安全监测系统，对接入应用安全隐患进行监测、防护和管理，确保安全接入与系统接入网部分的安全；对接入网与企业内网之间从物理层到应用层所有层次的通信协议进行隔离，为每一个允许的应用建立和维护一个专用数据交换机制，限定数据交换的源、目的、数据格式、数据内容，并对数据交换进行监控；

[0034] 安全接入平台层：为对外信息发布、信息采集、数据交换的中间区域，是接入终端网络连接的终点，所有应用访问终止于安全认证网关；安全接入平台层对交换业务注册、运行情况进行安全检测与审计，对网络设备、安全设备的配置管理及日常运行维护，对安全策略管理、流量监测、统计分析、安全审计，并以友好及人性化界面进行展示。

[0035] 移动应用层：用于支持移动终端的业务应用，实现系统的应用安全。

[0036] 所述的安全接入平台层设有接入网关、数据过滤交换系统、身份认证服务器及接入平台集中监控管理系统。

[0037] 为区别对待各接入的设备，所述的接入网关包括用于笔记本接入的安全接入网关、用于PDA/智能手机接入的移动安全接入网关、用于表计接入的表计安全接入网关。

[0038] 当智能终端为平板电脑、PDA或智能手机时，安全终端层使用的安全算法私钥或者数字证书采用MicroSD卡进行存储；在智能终端上设SIM卡，通过绑定专用APN的SIM卡实现网络通道安全；并在智能终端部署安全专控软件，实现安全通道建立、用户认证管理。

[0039] 移动应用层设移动应用服务器，应用服务器部署防病毒模块，保证应用服务区各应用服务器不被病毒、木马感染，防止病毒的传播和非法控制。

[0040] 图2所示，营销移动应用安全防护层次图主要内容包括：

[0041] 1)安全接入是整个平台的核心，第三方网络与企业信息网络之间构建安全接入区，进行网络的安全分隔。通过平台的安全接入、认证、访控服务等进行安全接入。

[0042] 2)通过建立不依赖于第三方运营商的二次加密隧道，增强数据传输安全性，而是经过安全接入区，进行用户身份的认证(数字证书系统)、数据加密(加密算法使用国密局专用安全算法，密码运算强度高，数据安全能得到有效保证)、用户数据的审计/授权、文件的在线加密。

[0043] 3)VPN网关接入服务层是核心部分，主要包括安全接入网关系统、身份认证系统、数据加解密、集中监控管理用户等逻辑功能组件，功能组件之间通过高速消息总线进行通信，实现各种安全服务。

[0044] 4)根据用户需求差异、应用差异、网络改造需求等，安全接入平台系统功能组、数据安全护系统等功能组件，可按照接入平台思想进行分段式组合部署，并进行网络层的无缝对接。

[0045] 5)身份认证系统，终端与VPN实行双向认证，并且通过CA服务认证授权。数字证书保障登陆安全平台系统的用户，都是通过管理认证的用户。数字证书的发放、撤销、过期重申请，既可以通OCSP协议在线方式；又可以通过离线的方式，由专人手动管理。

[0046] 6)防火墙，安全平台的接入边界，这是用户进入安全平台的首个对数据的安全过滤。防火墙是一种综合性的技术，涉及到计算机网络技术、密码技术、安全技术、软件技术、安全协议等多方面；是一种网络安全的保障手段；是网络通信时执行的一种访问控制尺度，其主要目标就是通过控制入、出一个网络的权限，并迫使所有的链接都经过这样的检查。

[0047] 所有的外部(用户)数据到内部(企业内网)的业务流均要经过防火墙，利用防火墙的网络地址翻译的功能和数据的安全过滤，对需要保护的网络进行保护。

[0048] 7)安全接入网关

[0049] IPSEC VPN接入网关，为用户远程访问网络服务提供安全保护，主要功能包括：

[0050] 身份认证：配合数字证书体系，确保远程访问者不是恶意用户；

[0051] 访问控制：确保访问者只能访问被授权访问的服务和信息；

[0052] 数据加密：配合SDKey中提供的商密算法，确保所有数据在网络传输过程中都是被加密的，防止被破解；

[0053] SSL VPN接入网关，为用户远程访问网络服务提供安全保护，主要功能包括：

[0054] 身份认证:配合数字证书体系,确保远程访问者不是恶意用户;

[0055] 访问控制:确保访问者只能访问被授权访问的服务和信息;

[0056] 数据加密:配合SDKey中提供的商密算法,确保所有数据在网络传输过程中都是被加密的,防止被破解。

[0057] 8)安全隔离系统

[0058] 安全隔离与信息交换系统,俗称“网闸”,网络隔离技术的目标是确保把有害的攻击隔离,在可信网络之外和保证可信网络内部信息不外泄的前提下,完成网间数据的安全交换。网络隔离技术是在原有安全技术的基础上发展起来的,它弥补了原有安全技术的不足,突出了自己的优势,它是安全子网与企业内网的安全隔离系统,保障访问业务内网的安全。

[0059] 9)审计、授权系统

[0060] 安全审计系统通过网络数据的采集、分析、识别,实时动态监测通信内容、网络行为和网络流量,发现和捕获各种敏感信息、违规行为,实时报警响应,全面记录网络系统中的各种会话和事件,实现对网络信息的智能关联分析、评估及安全事件的准确全程跟踪定位,为整体网络安全策略的制定提供权威可靠的支持。安全审计系统具有三大功能:

[0061] a、内容审计

[0062] SAS系统提供深入的内容审计功能,可对网站访问、邮件收发、远程终端访问、数据库访问、数据传输、文件共享等提供完整的内容检测、信息还原功能;并可自定义关键字库,进行细粒度的审计追踪。

[0063] b、行为审计

[0064] SAS系统提供全面的网络行为审计功能,根据设定行为审计策略,对网站访问、邮件收发、数据库访问、远程终端访问、数据传输、文件共享、网络资源滥用(即时通讯、论坛、在线视频、P2P下载、网络游戏等)等网络应用行为进行监测,对符合行为策略的事件实时告警并记录。

[0065] c、流量审计

[0066] SAS系统提供基于协议识别的流量分析功能,实时统计出当前网络中的各种报文流量,进行综合流量分析,为流量管理策略的制定提供可靠支持。

[0067] 安全通道层、安全接入平台层、移动应用开发平台组成移动作业平台,移动作业平台的搭建部署,主要包括如下:

[0068] 平台的信息安全与防护,包括国家电网公司安全接入平台支撑、应用服务的报文加密通讯、移动终端的数据库安全加密。

[0069] 跨平台的业务支撑,支持支持多种移动终端操作系统。如:ios,windowmobile,windowce,android,windowsxp,通过支持多种操作系统,同时建立一套统一规范的API,来适应各操作系统来实现跨平台的支持;支持各种终端硬件,如iphone,ipad,各种型号的android手机,各种型号的android平板,各种型号的windowsmobile/wince、pad。

[0070] 应用支撑功能,包括硬件底层支撑:打印、位置服务、条码扫描、高射频卡读写、用户电子签名认证、移动终端网络状态通知、其他硬件特性封装等;配备设备的审计登陆、用户登陆审计及服务组件的审计登陆认证;配备视频文件、图像文件、图案管理系统集成等文件服务功能;任务数据发布、下载、导入审核功能;用户认证及安全策略管理功能。

[0071] 移动GIS的支撑功能，基于国家电网公司GIS服务平台的支撑及地理图形展示、电网资源展示、GIS空间分析、路径导航、位置上报等功能。

[0072] 移动工作流支撑功能，包括电力移动应用发布平台服务端、客户端的管理。

[0073] 平台管理功能，包括设备管理、权限管理、业务菜单管理、移动终端的状态监控、服务监控及标准化现场作业分析功能。

[0074] 利用九种技术手段保障应用性能高效、稳定、可靠，独立设计业务表，存储用户、权限等信息；异步任务调度，实现工作单信息高效率实时下载；工作单流程信息通过短信实时推送，减轻人工刷新对系统的冲击；独立设计业务表，存储移动作业终端工作单信息；移动作业环节可参数化配置，控制业务影响范围；工作单业务数据下载可异步，最大化减少对BOSS专业系统冲击；作业数据上传可异步，提高数据传输成功率；批量工作单可拆分上传，减少单次上传的数据量，结构化数据与非结构化数据分开处理，提高数据上传效率。

[0075] 数据保存及与电力上位机的专业BOSS系统的实时数据交互采用双向互通的数据通道，数据传输的格式采用JSON数据传输，多媒体文件则通过FTP服务传输的方式实现。

[0076] 信息安全通过国网公司认证的安全接入平台进行保障，安全接入系统部署主要分为：企业端部署安全网关设备、安全终端内置定制加密芯片、企业自有两级CA系统、数据加密采用SM1算法、数字证书采用SM2算法、利用IPSEC/SSL VPN技术做数据通道的加密协议。

[0077] 以上图1、2所示的电力营销移动应用安全防护系统是本发明的具体实施例，已经体现出本发明实质性特点和进步，可根据实际的使用需要，在本发明的启示下，对其进行形状、结构等方面的等同修改，均在本方案的保护范围之列。

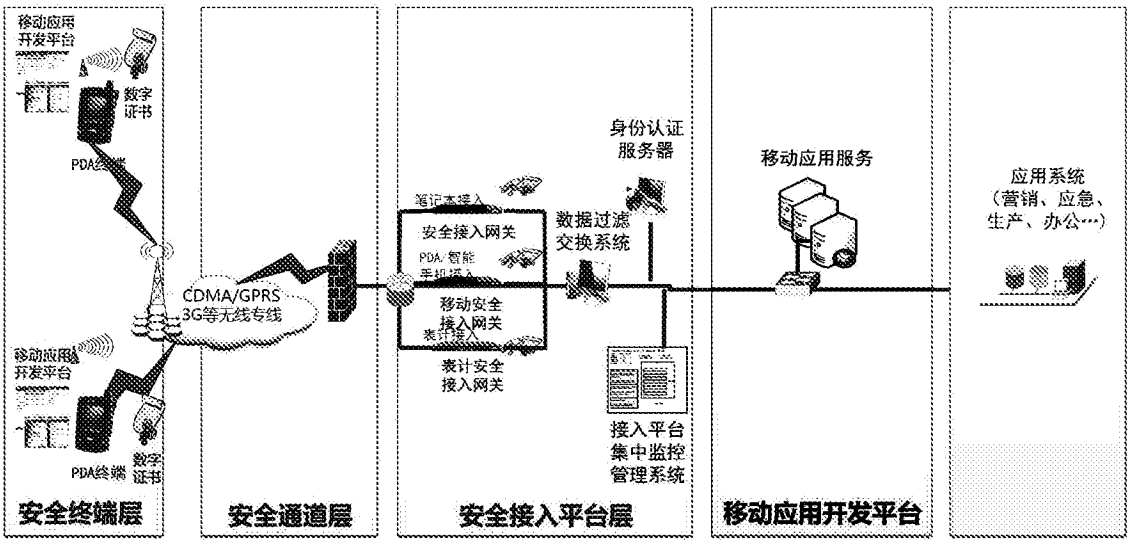

移动应用开发平台
数字证书
PDA终端
CDMA/GPRS
3G等无线专线
移动应用开发平台
PDA终端
数字证书
安全终端层
安全通道层
笔记本接入
安全接入网关
PDA/智能手机接入
移动安全接入网关
表计接入
表计安全接入网关
身份认证服务器
数据过滤交换系统
接入平台集中监控管理系统
安全接入平台层
移动应用服务
移动应用开发平台
应用系统（营销、应急、生产、办公…）

图1

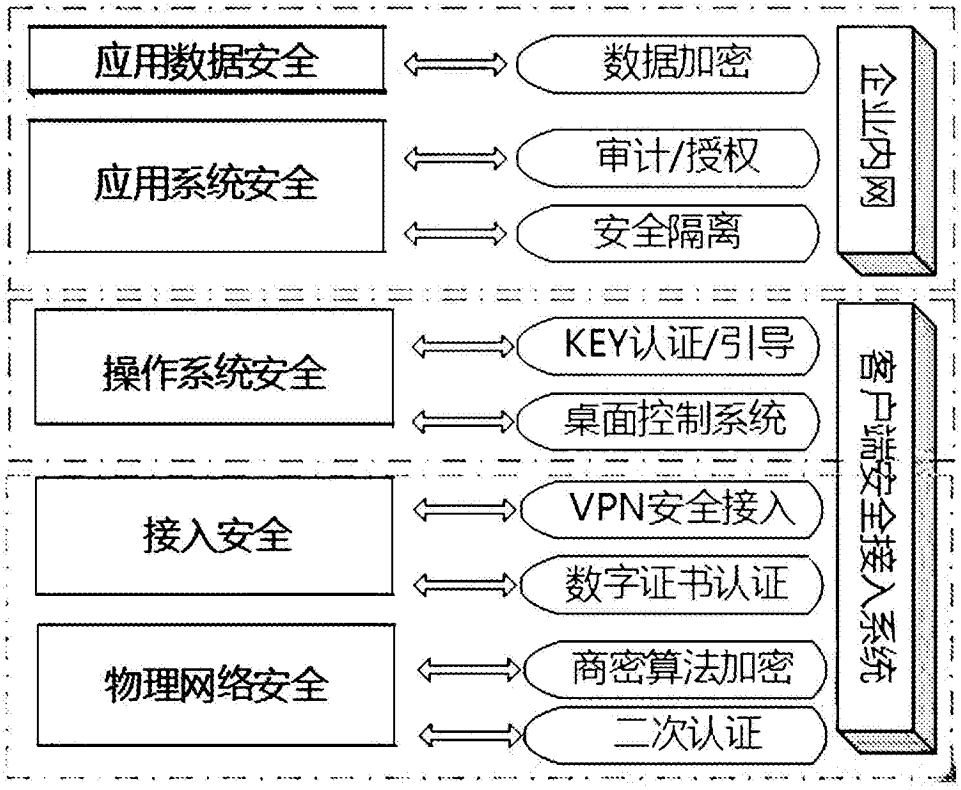

应用数据安全
数据加密
应用系统安全
审计/授权
安全隔离
企业内网
操作系统安全
KEY认证/引导
桌面控制系统
接入安全
VPN安全接入
数字证书认证
物理网络安全
商密算法加密
二次认证
客户端安全接入系统

图2