(19)中华人民共和国国家知识产权局

(12)发明专利申请

(10)申请公布号 CN 106992984 A
(43)申请公布日 2017.07.28

(21)申请号 201710211765.3

(22)申请日 2017.04.01

(71)申请人 国网福建省电力有限公司
地址 350003 福建省福州市鼓楼区五四路257号
申请人 国家电网公司
国网福建省电力有限公司信息通信分公司

(72)发明人 郭蔡炜 连纪文 周晟 蒋鑫 粟仁杰 程修远 郑飘飘 纪文 黄泽文

(74)专利代理机构 福州元创专利商标代理有限公司 35100
代理人 蔡学俊

(51)Int.Cl.
H04L 29/06(2006.01)

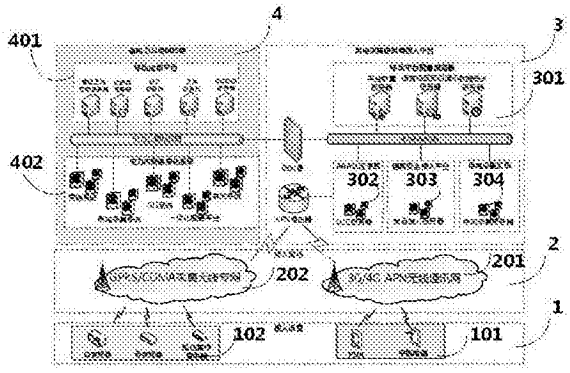
权利要求书2页 说明书4页 附图1页

(54)发明名称

一种基于电力采集网的移动终端安全接入信息内网的方法

(57)摘要

本发明涉及一种基于电力采集虚拟网的移动终端接入电力信息内网的方法，满足各种移动终端(平板电脑、PDA、智能手机等)访问电力企业信息内网的安全接入需求，利用成熟的电力采集虚拟网，对电力网络信息内网的应用平台进行防护，有效解决了非电力企业信息内网区域的移动终端、信息采集终端应用以安全专网方式接入信息内网的问题。



CN 106992984 A

1.一种基于电力采集网的移动终端安全接入信息内网方法，其特征在于，包括：并按照如下步骤实现：

步骤S1：对移动终端进行安全固化；在所述移动终端搭载一移动端安全专控平台，并通过该移动端安全专控平台进行接入；

步骤S2：移动终端网络接入；通过电力采集虚拟网提供的网络通道，移动终端通过3G/4G网络，以无线专网 APN 的方式安全接入所述；

步骤S3：通过所述电力采集虚拟网提供接入平台；接入平台包括：移动平台前置服务器、AAA认证系统、国网安全接入平台以及用电采集系统；

步骤S4：电力内网信息交互；通过千兆的防火墙作为移动作业平台服务器与电力信息内网互访的安全防护边界，采用静态NAT的地址映射方式，提供地址的一对一映射。

2.根据权利要求1所述的一种基于电力采集网的移动终端安全接入信息内网方法，其特征在于，在所述步骤S1中，所述移动终端内置密码卡，统一提供安全密码服务，存储有个人数字身份证书和签名私钥，用于数字签名、签名验证和数据加解密；所述密码卡内采用商用密码分组算法SM1进行数据加密传输，支持RSA、ECC公钥密码算法，作为网络客户端信息安全识别载体，提供标准的CSP服务，支持PKCS系列标准。

3.根据权利要求1所述的一种基于电力采集网的移动终端安全接入信息内网方法，其特征在于，所述移动终端包括：PDA、智能平板以及智能手机。

4.根据权利要求1所述的一种基于电力采集网的移动终端安全接入信息内网方法，其特征在于，在所述步骤S2中，所述移动终端通过无线专网APN接入所述电力采集虚拟网；所述无线专网APN支持多种加密算法，并允许用户添加额外的第三方算法，采用国密办认证算法SCB2以及SM1，采用面向用户的数字证书认证、USB－Key认证、短信认证以及动态令牌认证，通过数字证书认证，保证用户接入时的身份安全与权限安全。

5.根据权利要求1所述的一种基于电力采集网的移动终端安全接入信息内网方法，其特征在于，在所述步骤S3中，所述移动平台前置服务器包括：平台前置服务器、语言视频即时服务器以及通讯数据同步服务器；所述AAA认证系统包括一认证服务器；所述国网安全接入平台包括一安全接入服务器；所述用电采集系统包括一用电采集服务器。

6.根据权利要求5所述的一种基于电力采集网的移动终端安全接入信息内网方法，其特征在于，所述AAA认证系统与所述国网安全接入平台包括：安全接入网关系统组件、身份认证系统组件、数据加解密组件以及集中监控管理用户组件，各功能组件之间通过高速消息总线进行通信，提供安全服务。

7.根据权利要求6所述的一种基于电力采集网的移动终端安全接入信息内网方法，其特征在于，所述安全接入网关系统组件为用户远程访问网络服务提供安全保护，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.根据权利要求6所述的一种基于电力采集网的移动终端安全接入信息内网方法，其特征在于，所述身份认证系统组件提供AAA身份认证；移动终端与所述无线专网APN实行双向认证，并且通过CA服务认证授权；数字证书通过管理认证的用户；通过OCSP协议在线方

式，对数字证书进行发放、撤销以及过期重申请；或通过离线的方式，由专人手动管理。

9.根据权利要求1所述的一种基于电力采集网的移动终端安全接入信息内网方法，其特征在于，在所述步骤S4中，所述移动终端提供的所有外部数据经过所述防火墙传输至所述电力信息内网，通过所述防火墙对外部数据进行网络地址翻译以及数据安全过滤。

10.根据权利要求1所述的一种基于电力采集网的移动终端安全接入信息内网方法，其特征在于，在所述步骤S4中，所述电力信息内网包括：移动应用平台与电力内网信息化系统；所述移动应用平台包括：移动平台服务器、文件服务器、GIS功能服务器、管理主站应用服务器、接口服务器以及数据库服务器；所述电力内网信息化系包括：电力营销系统、用电采集系统、GIS系统以及一体化缴费平台。

一种基于电力采集网的移动终端安全接入信息内网的方法

技术领域

[0001] 本发明涉及电力营销领域，特别是一种基于电力采集虚拟网的移动终端接入电力信息内网的方法。

背景技术

[0002] 国家电网在电力营销信息化工作不断深化的过程中，移动应用在营销业务管理中逐步展开。如何保证各类移动终端安全、可信地连入电力信息内网，已成为移动应用能否全面展开的关键性因素。

[0003] 为确保信息安全，国家电网提出“双网隔离、双网双机”的政策，即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，要求员工必须用不同的计算机接入内网与外网。该举措有效地提升了信息安全水平，但由于内网接入条件严格，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。

[0004] 国家电网在移动安全接入方面还提出国网安全接入平台方案，为移动作业在电力营销的深化应用提供基础保障。然而，在通信稳定性、安全性、大量终端并发性和经济性方面，当前的移动终端安全接入方法上还有进一步提升的空间。

发明内容

[0005] 本发明的目的在于提供一种基于电力采集网的移动终端安全接入信息内网方法，以克服现有技术中存在的缺陷。

[0006] 为实现上述目的，本发明的技术方案是：一种基于电力采集网的移动终端安全接入信息内网方法，包括：并按照如下步骤实现：

步骤S1：对移动终端进行安全固化；在所述移动终端搭载一移动端安全专控平台，并通过该移动端安全专控平台进行接入；

步骤S2：移动终端网络接入；通过电力采集虚拟网提供的网络通道，移动终端通过3G/4G网络，以无线专网 APN 的方式安全接入所述；

步骤S3：通过所述电力采集虚拟网提供接入平台；接入平台包括：移动平台前置服务器、AAA认证系统、国网安全接入平台以及用电采集系统；

步骤S4：电力内网信息交互；通过千兆的防火墙作为移动作业平台服务器与电力信息内网互访的安全防护边界，采用静态NAT的地址映射方式，提供地址的一对一映射。

[0007] 在本发明一实施例中，在所述步骤S1中，所述移动终端内置密码卡，统一提供安全密码服务，存储有个人数字身份证书和签名私钥，用于数字签名、签名验证和数据加解密；所述密码卡内采用商用密码分组算法SM1进行数据加密传输，支持RSA、ECC公钥密码算法，作为网络客户端信息安全识别载体，提供标准的CSP服务，支持PKCS系列标准。

[0008] 在本发明一实施例中，所述移动终端包括：PDA、智能平板以及智能手机。

[0009] 在本发明一实施例中，在所述步骤S2中，所述移动终端通过无线专网APN接入所述

电力采集虚拟网;所述无线专网APN支持多种加密算法,并允许用户添加额外的第三方算法,采用国密办认证算法SCB2以及SM1,采用面向用户的数字证书认证、USB－Key认证、短信认证以及动态令牌认证,通过数字证书认证,保证用户接入时的身份安全与权限安全。

[0010] 在本发明一实施例中,在所述步骤S3中,所述移动平台前置服务器包括:平台前置服务器、语言视频即时服务器以及通讯数据同步服务器;所述AAA认证系统包括一认证服务器;所述国网安全接入平台包括一安全接入服务器;所述用电采集系统包括一用电采集服务器。

[0011] 在本发明一实施例中,所述AAA认证系统与所述国网安全接入平台包括:安全接入网关系统组件、身份认证系统组件、数据加解密组件以及集中监控管理用户组件,各功能组件之间通过高速消息总线进行通信,提供安全服务。

[0012] 在本发明一实施例中,所述安全接入网关系统组件为用户远程访问网络服务提供安全保护,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。

[0013] 在本发明一实施例中,所述身份认证系统组件提供AAA身份认证;移动终端与所述无线专网APN实行双向认证,并且通过CA服务认证授权;数字证书通过管理认证的用户;通过OCSP协议在线方式,对数字证书进行发放、撤销以及过期重申请;或通过离线的方式,由专人手动管理。在本发明一实施例中,在所述步骤S4中,所述移动终端提供的所有外部数据经过所述防火墙传输至所述电力信息内网,通过所述防火墙对外部数据进行网络地址翻译以及数据安全过滤。在本发明一实施例中,在所述步骤S4中,所述电力信息内网包括:移动应用平台与电力内网信息化系统;所述移动应用平台包括:移动平台服务器、文件服务器、GIS功能服务器、管理主站应用服务器、接口服务器以及数据库服务器;所述电力内网信息化系包括:电力营销系统、用电采集系统、GIS系统以及一体化缴费平台。

[0014] 相较于现有技术,本发明具有以下有益效果:本发明所提出的一种基于电力采集网的移动终端安全接入信息内网方法,充分利用电力现有网络资源和IT基础设施,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。

附图说明

[0015] 图1为本发明中基于电力采集网的移动终端安全接入信息内网的方法安全防护结构示意图。

具体实施方式

[0016] 下面结合附图,对本发明的技术方案进行具体说明。

[0017] 本发明提供一种基于电力采集网的移动终端安全接入信息内网的方法过程,包

括:移动终端安全固化1、移动终端网络接入2、用电采集虚拟网接入平台3和内网信息交互4。

[0018] 进一步的,移动终端安全固化。主要针对移动终端101进行专控安全软件安装固化,移动终端101包括的类型有PDA、智能平板、智能手机等。移动终端的安全算法私钥或者数字证书采用MicroSD卡(TF卡)进行存储,适合平板电脑、PDA、智能手机。移动终端的网络通道安全,通过绑定专用APN的SIM卡,进一步提高信息通讯安全。移动终端部署安全专控软件,实现安全通道建立、用户认证管理。

[0019] 进一步的,安全固化还包括终端操作系统固化,登录密码加密等。移动终端内置密码卡,统一提供安全密码服务,可存储个人数字身份证书和签名私钥,实现数字签名、签名验证和数据加解密等密码服务。密码卡内采用当前主流的商用密码分组算法SM1进行数据加密传输,支持RSA、ECC公钥密码算法,可用作网络客户端信息安全识别载体,能提供标准的CSP服务,支持PKCS系列标准。移动终端通过按照安全专控软件,登录安全接入管理平台

进一步的,移动终端网络接入。包括移动终端101接入的3G/4G APN无线通讯网201和电力采集终端(公变终端、专变终端、低压集中器)接入的GPRS/CDMA采集无线专网。利用电力采集虚拟网提供的网络通道,移动终端可通过3G/4G网络以无线专网 APN 的方式进行安全接入。移动终端直接通过APN连接,通过防火墙接入,可以从安全、速度、操作性等方面保证用户接入网络的效率。APN支持多种加密算法,并允许用户添加额外的第三方算法,采用国密办认证算法(SCB2、SM1),从传输机制上保障数据传输时的安全。面向用户的数字证书认证、USB—Key认证、短信认证、动态令牌认证等多种安全认证手段,通过数字证书认证,保证用户接入时的身份安全与权限安全。

[0020] 进一步的,用电采集虚拟网接入平台3,包括移动平台前置服务器301、AAA认证系统302、国网安全接入平台303、用电采集系统304。用电采集虚拟网接入平台3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。

[0021] 在移动终端与用电采集虚拟网接入平台之间,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。

[0022] 用电采集虚拟网接入平台,以“认证、三层网络、多次数据保护”的体系结构为主线,在各个节点使用各种安全设备和体系,对移动终端的接入做全方位的保护,并使访问各个应用服务系统以最好的支持。用电采集虚拟网接入平台包括移动平台前置服务器、AAA认证系统、国网安全接入平台、用电采集系统。利用采集虚拟专网的安全防护体系,采用运营商接入防火墙防止外部非法的接入。部署入侵防御系统,对网络流量进行实时监测,抵御外部的蠕虫、病毒、间谍软件和黑客的攻击以及基于应用层的非法入侵等。利用互备的AAA服务器实现对外部移动作业终端进行身份认证,进一步保证了从运营商网络接入到专网内部的安全性。

[0023] 进一步的,AAA认证系统和国网安全接入平台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。

[0024] 根据用户需求差异、应用差异、网络改造需求等，用电采集虚拟网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。

[0025] AAA身份认证系统，终端与APN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，即可以通OCSP协议在线方式；又可以通过离线的方式，由专人手动管理。.

国网安全接入网关，为用户远程访问网络服务提供安全保护，主要功能包括：

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。

[0026] 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。

[0027] 进一步的，内网信息交互，利用千兆防火墙作为移动作业平台服务器与信息内网(例如营销系统)互访的安全防护边界，采用静态NAT的地址映射方式，提供地址的一对一映射。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。

[0028] 本发明利用专门用于电力营销用电信息采集系统数据采集的无线网络采集虚拟网，移动终端可通过3G/4G网络以无线专网 APN 的方式进行安全接入，再通过移动运营商NAS认证转发之后进入AAA认证服务器并且获取到IP，从而保证终端接入的安全性。以现有的用电信息采集虚拟网为基础，充分利用现有采集虚拟网的网络平台和安全防护的资源，确保移动终端的接入对象安全、可信地接入电力信息网络，同时保证机密数据不会泄露，并且实现对接入对象和操作的细粒度监控与审计。基于电力采集虚拟网的移动终端接入电力信息内网的方法，依托先进的安全认证体系，实现对移动终端的统一接入、认证、授权、计费与管理，实现电力营销相关的移动作业现场服务应用，使移动作业更加安全、可靠，从技术上支持提升企业集约化、精益化和标准化管理水平的管理要求。

[0029] 进一步的，基于电力采集虚拟网的移动终端接入电力信息内网方法的优点是，电力采集虚拟网已经运行较长的时间，且目前已建成移动、联通、电信三个运营商的网络接入通道，设备通过AAA系统进行认证接入，很好的保证通信的安全性；另外具有成本低的特点，采集虚拟网的安全认证平台是已有系统，不需要再进行二次开发。

[0030] 以上是本发明的较佳实施例，凡依本发明技术方案所作的改变，所产生的功能作用未超出本发明技术方案的范围时，均属于本发明的保护范围。

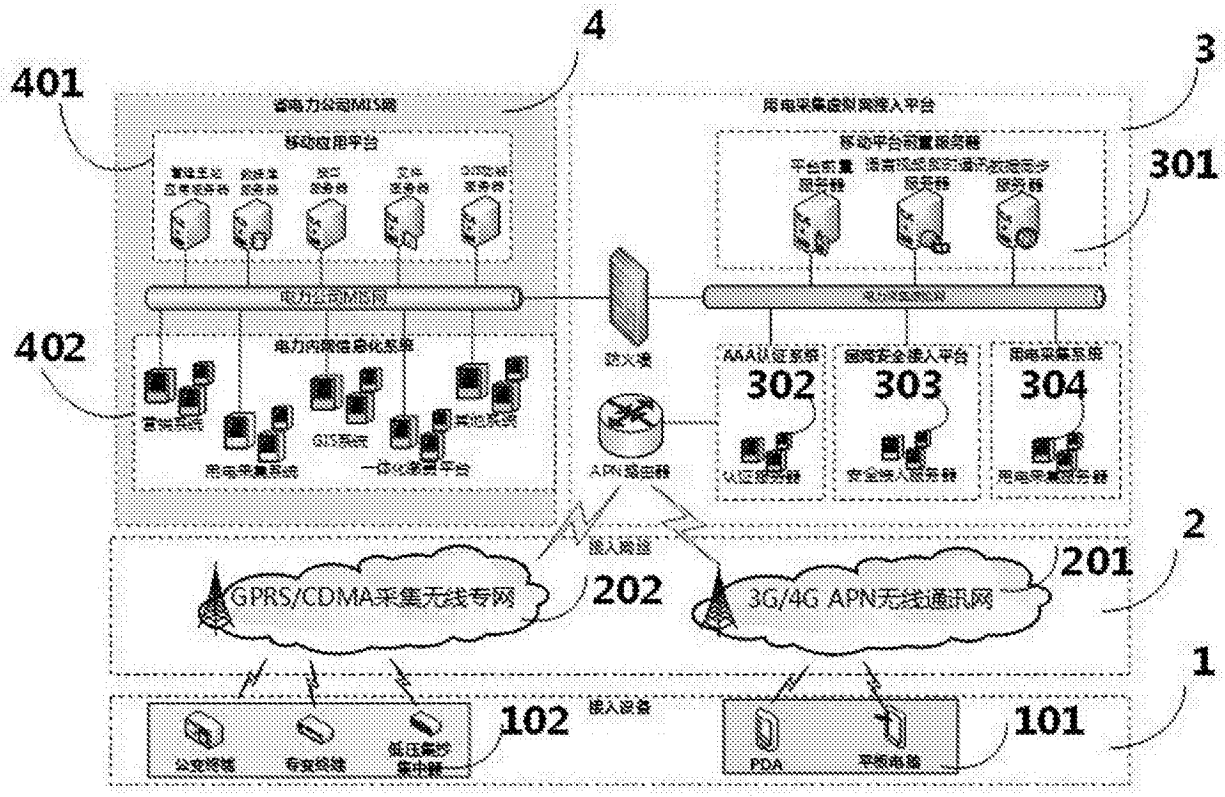

4
401
3
301
402
302
303
304
APN通信网
GPRS/CDMA采集无线专网
202
3G/4G APN无线通讯网
201
2
1
102
101
PDA

图1