ICS 29.240.30
F 21
备案号：53932-2016

DL

# 中华人民共和国电力行业标准

DL / T 1511 — 2016

# 电力系统移动作业 PDA 终端安全防护技术规范

**Security protection technical specification for power system mobile operation PDA**

2016-01-07发布　　2016-06-01实施

国家能源局　发布

# 目　　次

# 前　言

本标准依据 GB/T 1.1—2009 给出的规则起草。

本标准由中国电力企业联合会提出。

本标准由全国电力系统管理及其信息交换标准化技术委员会（SAC/TC 82）归口。

本标准起草单位：全球能源互联网研究院（原国网智能电网研究院）、国网电力科学研究院、中国电力科学研究院、国网上海市电力公司、国网江苏省电力公司。

本标准主要起草人：陈亚东、张涛、林为民、邵志鹏、楚杰、马媛媛、郭经红、曾荣、时坚、王玉斐、蒋诚智、费稼轩、戴造建。

本标准在执行过程中的意见或建议反馈至中国电力企业联合会标准化管理中心（北京市白广路二条一号，100761）。

# 电力系统移动作业 PDA 终端
# 安全防护技术规范

## 1 范围

本标准规定了电力系统移动作业 PDA 终端安全防护遵循的主要技术原则和技术要求。本标准描述的电力系统移动作业 PDA 终端，是通过无线 APN/VPDN 网络接入移动作业业务系统的 PDA 终端。

本标准适用于接入移动作业系统进行移动作业的 PDA 终端的安全防护，在 PDA 终端安全防护的设计、开发、实施和检测时可参照执行。

## 2 术语和定义

下列术语和定义适用于本文件。

2.1

**PDA 终端　Personal Digital Assistant (PDA) terminal**

一种小型便携式终端设备，一般安装移动操作系统如 Android、Windows mobile 等，可以进行无线通信，PDA 在电力移动作业业务系统中得到广泛应用。

2.2

**接入点　Access Point Name (APN)**

无线网络服务运营商提供的无线专线网络服务，企业租用的 APN 的无线节点可以互相通信，而不能和其他专用无线网络通信。

2.3

**虚拟专用拨号网　Virtual Private Dial-up Networks (VPDN)**

无线网络服务运营商提供的无线虚拟专用拨号网业务，无线服务用户可以接入无线虚拟专用拨号网，实现无线网络专用。

2.4

**移动作业　mobile operation**

采用移动终端通过无线 APN/VPDN 方式接入电力业务系统主站进行现场在线作业的业务应用模式，终端运行电力业务应用软件，生产人员在现场使用终端与电力业务系统进行在线双向数据交换。

2.5

**数字证书　digital certificate**

数字证书是由权威证书授权中心发放的标识证书所有者身份的电子身份凭证和电子签章载体，主要包括三方面的内容：证书所有者的信息、证书所有者的公开密钥、证书颁发机构的签名，数字证书采用公钥密码体制对传输数据进行加密解密、数字签名和验证，确保数据的机密性、完整性，以及证书所有者身份的真实性和不可否认性。

2.6

**身份认证　identity authentication**

对用户身份标识的有效性进行验证的过程。

2.7

**对称密钥　secret key**

用于对称密码算法的密钥。

2.8

**对称密码算法　symmetric cryptographic algorithm**

加解密使用相同密钥的密码算法，数据传输双方使用相同的密钥加密和解密。

2.9

**非对称密码算法　asymmetric cryptographic algorithm**

加解密使用非对称的公钥和私钥的算法。公钥和私钥组成一对非对称密钥，用公钥加密的数据只有对应的私钥可以解密，用私钥加密的数据只有对应的公钥可以解密，其中公钥可以公开，私钥必须保密，由公钥求解私钥是计算不可行的。

2.10

**RSA 算法　Rivest-Shamir-Adleman algorithm (RSA)**

一种基于大整数因子分解问题的公钥密码算法。

2.11

**SM1 算法　SM1 algorithm**

一种分组密码算法，分组长度为 128 bit，密钥长度为 128 bit。

2.12

**SM2 算法　SM2 algorithm**

一种椭圆曲线公钥密码算法。

2.13

**安全 TF 卡　security TF card**

T-Flash 卡，又名 Micro SD 卡，是一种利用 Micro SD 接口使用的存储卡，移动终端常见存储设备，安全 TF 集成了支持国家密码管理局标准 SM1、SM2 算法的密码芯片，具有对称、非对称加解密功能，可以通过配套安全模块调用密码算法，并支持数字证书解析，支持数据分区分域和加密存储。

2.14

**安全模块　security module**

安全模块是以安全 TF 卡为基础，实现调用硬件密码运算的软件模块，安装在移动作业 PDA 终端上，是 PDA 安全防护的软件支撑，安全模块调用安全 TF 卡的算法，为运行在终端上的电力业务软件提供安全防护服务，具有数据加密存储、数据传输加解密、网络访问控制、进程控制等安全功能。

2.15

**白名单　white list**

允许通过的用户、业务（如应用程序、进程、IP 地址、IP 包、数据访问端口等）等对象的名单。白名单内的对象可以通过，白名单以外的对象不能通过。

## 3　总体防护要求

为了消除移动作业 PDA 终端面临的风险（见附录 A），移动作业 PDA 终端上安装安全模块和安全 TF 卡，实现对终端接入主站整个过程中的安全防护，终端防护措施包括安全 TF 卡、安全模块和业务软件的安全防护技术措施，如图 1 所示。

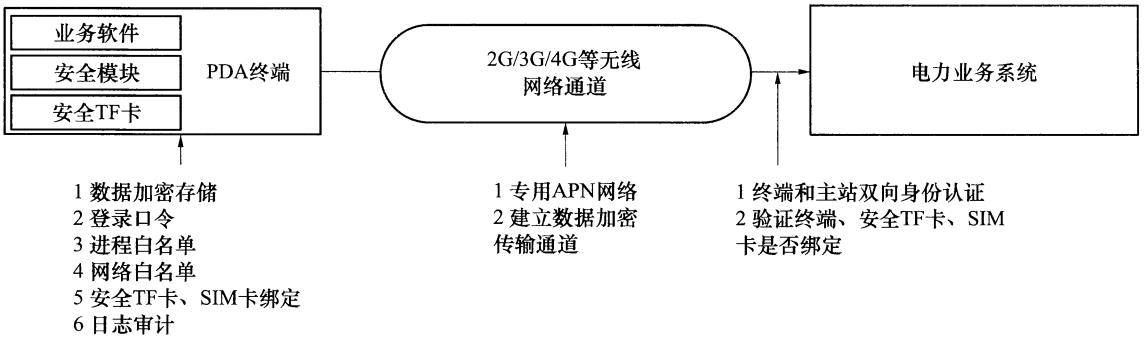


图 1　安全防护技术措施

## 4　防护功能

### 4.1　终端防护

#### 4.1.1　安全 TF 卡技术要求

安全 TF 卡应通过国家密码管理局密码认证，应符合以下技术要求：

a）　支持 SM1 对称密码算法；

b）　支持 SM2 非对称密码算法和 SM2 格式证书解析；

c）　支持数据分区隔离和数据加密存储。

#### 4.1.2　安全模块技术要求

安全模块技术要求包括：

a）　数据分区隔离和数据加密存储功能，应具有对业务软件数据、用户数据、系统配置数据、操作维护记录数据、日志审计数据分区加密存储功能；

b）　数据传输加解密功能，应支持将数据利用 SM1 对称密码算法加密功能；

c）　网络访问控制功能，应具有配置网络访问控制功能，非经配置允许的网络地址、端口不允许访问；

d）　进程控制功能，应具有配置进程控制功能，非经配置允许的进程不能启动；

e）　终端安全审计功能，应对安全模块运行异常、安全 TF 卡运行异常、访问进程白名单之外的进程、访问网络白名单之外的网络情况记录日志。

#### 4.1.3　业务软件技术要求

业务软件应支持以下功能：

a）　口令认证：在启动时进行登录口令认证；

b）　文件检查：检查自身文件是否缺失或被非法篡改，应在启动时检查配置是否被修改；

c）　数据备份：关键数据在 TF 卡中加密备份；

d）　日志审计：记录业务访问异常情况。

### 4.2　网络防护

网络防护要求包括：

a）　终端使用的 SIM 卡应绑定开通的 APN/VPDN 网络，不允许访问其他 APN/VPDN 网络和互联网；

b） 应在终端和主站之间建立数据加密传输通道。

### 4.3 接入防护

业务软件启动时先调用安全模块，安全模块与主站侧进行基于数字证书的双向身份认证，认证成功后安全模块与主站建立加密通道，业务软件利用加密通道进行数据传输。

终端接入应按照图 2 所示的接入过程进行以下步骤的认证过程：

a） 客户端发起认证请求；
b） 服务端接受客户端的认证请求；
c） 服务端验证本地证书是否由指定机构颁发；
d） 服务端将公钥发送给客户端；
e） 客户端验证本地证书是否由指定机构颁发；
f） 客户端将公钥发送给服务端；
g） 服务端验证客户端身份正确；
h） 身份认证结束，建立加密通道；
i） 客户端和服务端双方根据双方的公钥计算出一个对称密钥；
j） 验证通过终端可以进行移动作业；
k） 客户端和服务端进行双向数据加密传输。

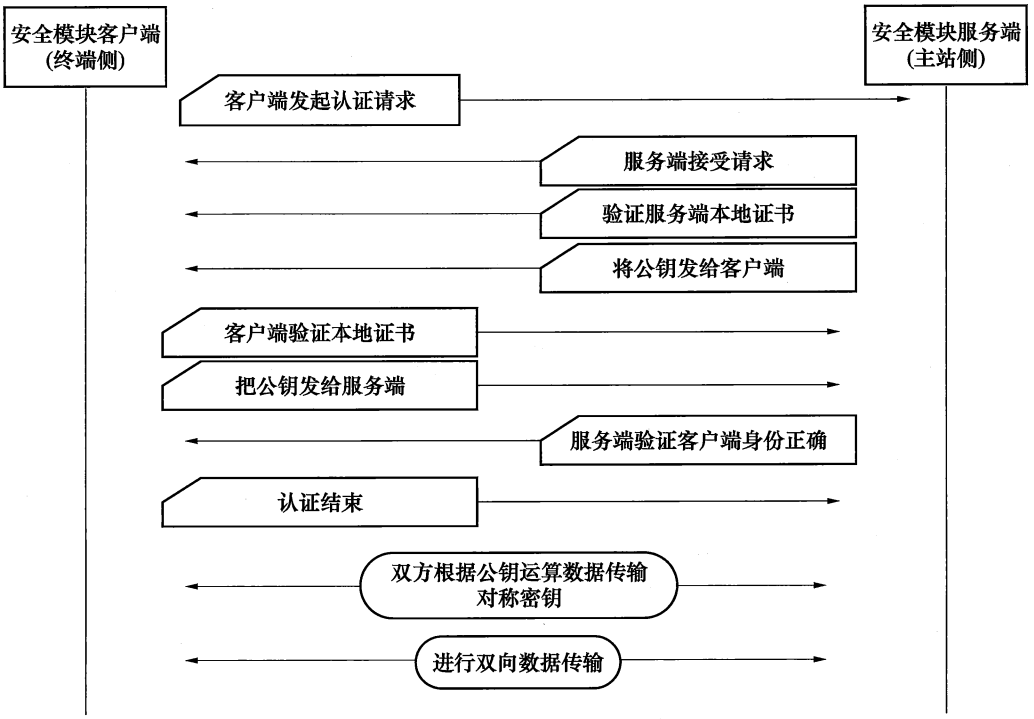


图 2 接入过程

## 5 安全检测

### 5.1 终端防护功能检测

#### 5.1.1 安全 TF 卡功能检测

本项检测包括：

a） 访问安全 TF 卡加密分区应提示输入密码；
b） 安全 TF 卡中数据应是密文，一般破解方法不能解密数据。

#### 5.1.2 安全模块功能检测

本项检测包括：
a） 在进程白名单中的进程应正常启动；
b） 进程白名单之外的进程不应启动；
c） 网络白名单中的网络应能访问；
d） 网络白名单之外的网络地址、端口应不能访问；
e） 安全模块的日志中应能查询到进程运行和网络访问记录。

#### 5.1.3 业务软件功能检测

本项检测包括：
a） 启动业务软件，输入正确口令应能打开，输入不正确口令应提示口令错误；
b） 修改、删除业务软件的文件，启动业务软件应提示文件被修改或者删除，无法启动；
c） 登录业务软件后，应能在操作菜单中查看业务数据及其备份；
d） 业务软件与主站失去连接时，应提示并记录日志。

### 5.2 网络防护功能检测

本项检测包括：
a） 终端启动业务软件，访问运营商提供的其他 APN/VPDN 网络的 IP 地址应不能访问；
b） 终端无访问互联网功能，并且使用端口扫描工具对运营商提供的专用 APN/VPDN 的服务端地址进行扫描，应不能访问到任何开放端口。

### 5.3 接入防护功能检测

本项检测包括：
a） 在终端导入颁发的数字证书，安全模块应能够与主站侧建立连接，终端应可以正常作业；
b） 更换不是给终端颁发的数字证书，安全模块应提示身份认证不成功并记录日志；
c） 更换安全 TF 卡或者 SIM 卡，主站侧应阻止接入，安全模块应提示无法与主站建立安全连接，并记录日志。

### 5.4 安全检测结果样例

参见附录 B。

# 附 录 A
（资料性附录）
业务应用环境与风险分析

在电力系统中广泛使用的移动作业 PDA 终端的应用环境如图 A.1 所示，终端上部署基于终端系统环境开发的移动作业软件，通过 2G/3G/4G 等无线网络通道，接入到电力业务主站，进行移动作业。

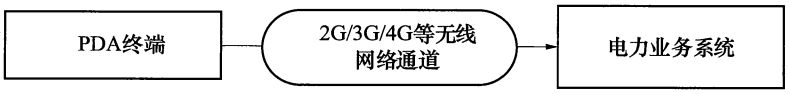


图 A.1 典型应用环境

在终端接入业务主站进行作业过程中，在 PDA 终端自身、网络通道、终端接入三个环节存在风险，如图 A.2 所示。

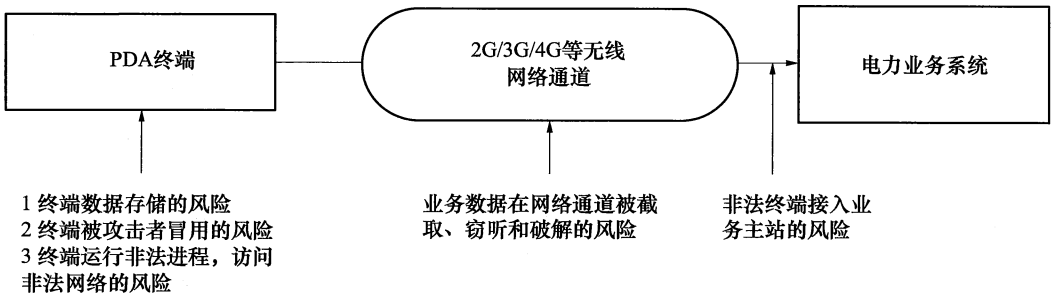


图 A.2 应用环境风险分析

# 附 录 B
（资料性附录）
安全检测结果样例

安全检测结果样例见表 B.1。

**表 B.1 安全检测结果样例**

| 检 测 内 容 | 检 测 结 果 |
| --- | --- |
| 安全 TF 卡功能检测 | 访问安全 TF 卡加密分区需要密码验证；<br>安全 TF 卡中数据无法通过常规工具读出 |
| 安全模块功能检测 | 配置进程白名单，白名单中的进程正常启动，非白名单之内的进程不能启动；<br>配置网络白名单，白名单中的网络应能访问，非白名单之内的网络不能访问；<br>查看安全模块日志，能查询到进程运行和网络访问的记录 |
| 业务软件功能检测 | 启动业务软件，提示输入密码；<br>在业务软件菜单中可以查看业务数据及其备份；<br>发起业务软件与主站连接，然后断开连接，查看日志，有连接成功和连接断开的日志 |
| 网络防护功能检测 | 启动业务软件，配置在运营商提供的 APN/VPDN 网络的 IP 地址之外的网络，开始连接，提示不能访问；<br>打开终端上的浏览器，访问互联网，提示不能访问 |
| 接入防护功能检测 | 在终端导入给颁发的数字证书，启动安全模块与主站侧建立连接，显示连接成功，业务软件正常作业；<br>更换不属于该终端的数字证书，启动安全模块，提示身份认证不成功，查看日志，有数字证书不匹配的记录；<br>更换安全 TF 卡或者 SIM 卡，启动安全模块与主站侧建立连接，安全模块提示无法连接主站，查看日志，有安全 TF 卡不匹配和 SIM 卡不匹配的记录 |

中 华 人 民 共 和 国
电 力 行 业 标 准
**电力系统移动作业 PDA 终端**
**安 全 防 护 技 术 规 范**
**DL / T 1511 — 2016**
*
中国电力出版社出版、发行
（北京市东城区北京站西街 19 号　100005　http://www.cepp.sgcc.com.cn）
北京传奇佳彩数码印刷有限公司印刷
*
2016 年 7 月第一版　　2016 年 7 月北京第一次印刷
880 毫米×1230 毫米　16 开本　0.75 印张　16 千字
印数 001—200 册
*
统一书号 155123・3020　定价 **9.00** 元

**敬 告 读 者**
本书封底贴有防伪标签，刮开涂层可查询真伪
本书如有印装质量问题，我社发行部负责退换
**版 权 专 有　翻 印 必 究**

中国电力出版社官方微信

掌上电力书屋

刮开涂层
查询真伪

155123.3020