

# DB4403

## 深圳市地方标准

DB4403/T XXX—XXXX

### 虚拟电厂终端授信及安全加密技术规范

(送审稿)

XXXX-XX-XX 发布

XXXX-XX-XX 实施

深圳市市场监督管理局 发布



目 次

目 次 ..... I

前 言 ..... II

1 范围 ..... 1

2 规范性引用文件 ..... 1

3 术语和定义 ..... 1

4 缩略语 ..... 3

5 总体目标及要求 ..... 3

6 网络安全要求 ..... 4

7 安全加密方式 ..... 5

8 安全加密要求 ..... 6

## 前 言

本文件按照GB/T 1.1—2020《标准化工作导则 第1部分：标准化文件的结构和起草规则》给出的规则起草。

本文件由深圳市发展和改革委员会提出并归口。

本文件主要起草单位：深圳供电局有限公司、南方电网科学研究院有限责任公司、深圳市科技创新委员会、深圳国家高技术产业创新中心、深圳市建筑科学研究院股份有限公司、深圳特来电新能源有限公司、南京德睿能源研究院有限公司、南方电网电动汽车有限公司、华为数字能源技术有限公司、万帮数字能源股份有限公司。

本文件主要起草人：程韧俐、索思亮、史军、李江南、王滔、杨帆、周保荣、赵文猛、陈立明、匡晓云、毛田、李蓉、左新兵、李林军、李雨桐、王冰、韩亚宁、刘杰、李勋、葛静、孙务本、牛雷、司宇峰。

# 虚拟电厂终端授信及安全加密技术规范

## 1 范围

本文件规范了虚拟电厂在终端身份认证及安全加密方面的总体目标及要求、网络安全要求、安全加密方式等技术要求。

本文件适用于虚拟电厂业务中进行安全加密和身份认证的虚拟电厂安全加密网关,安全加密终端及其他安全防护设备。

## 2 规范性引用文件

下列文件中的内容通过文中的规范性引用而构成本文件必不可少的条款。其中注日期的引用文件,仅该日期对应的版本适用于本文件;不注日期的引用文件,其最新版本(包括所有的修改单)适用于本文件。

- GM/T 0005—2021 随机数检测规范
- GM/T 0009—2012 SM2密码算法使用规范
- GM/T 0014—2012 数字证书认证系统密码协议规范
- GM/T 0015—2012 基于SM2密码算法的数字证书格式规范
- GM/T 0022—2014 IPSec VPN技术规范
- GM/T 0024—2014 SSL VPN技术规范
- GM/Z 0001—2013 密码术语
- GA/T 686—2018 信息安全技术 虚拟专用网产品安全技术要求
- GB/T 4208—2017 外壳防护等级(IP代码)
- GB/T 13729—2019 远动终端设备
- GB/T 15153.2—2000 远动设备及系统 第2部分:工作条件 第2篇 环境条件
- GB/T 22239—2019 信息安全技术 网络安全等级保护基本要求
- GB/T 36572—2018 电力监控系统网络安全防护导则
- GB/T 37934—2019 信息安全技术 工业控制网络安全隔离与信息交换系统安全技术要求
- DL/T 2473.2—2022 可调节负荷并网运行与控制技术规范 第2部分:网络安全防护
- Q/CSG 212001—2018 中国南方电网电力监控系统安全防护管理办法
- Q/CSG 1204009—2015 中国南方电网电力监控系统安全防护技术规范

## 3 术语和定义

### 3.1

**电力监控系统** Power Monitoring System

用于监视和控制电力生产及供应过程的、基于计算机及网络技术的业务系统及智能设备,以及作为基础支撑的通信及数据网络等。

### 3.2

### 3.3

**网络安全** Network Security

网络系统的硬件、软件及其系统中的数据受到保护，不因偶然的或者恶意的原因而遭受到破坏、更改、泄露，系统连续可靠正常地运行，网络服务不中断。

### 3.4

#### 虚拟电厂 Virtual Power Plant

通过先进信息通信技术和软件系统，实现分布式电源、储能系统、可控负荷、电动汽车等资源的聚合、协调优化与控制，可形成虚拟等效的对外功率调节服务，提供与传统电厂性能相匹配的电网运行支撑能力。

### 3.5

#### 虚拟电厂管理云平台 Virtual Power Plant Management Platform

基于调控机构调度控制系统平台部署的满足相关网络安全防护等级要求的，可接受调控业务平台，承担与聚合商平台间交互监视、控制和电力市场等相关数据的功能模块和系统级应用，是传统调度自动化系统功能的外延拓展，具备虚拟电厂接入管理、可调节能力评估、调控邀约发布与组织交易，出清计算、调度指令下发、自动功率控制、收益计算分配、资源统计查询等功能。

### 3.6

#### 可调节负荷 Adjustable Load

电力系统中具备技术条件并参与电网调节运行的负荷资源，通过负荷聚合平台接入的负荷资源。

**注：**常见的可调节负荷包括但不限于电动汽车（充电桩）、大工业用户负荷、空调机组、智能楼宇以及虚拟电厂聚合的各类负荷、部分中小型分布式新能源、中小型储能站等。

### 3.7

#### 直控负荷 Direct Control Load

不经过负荷聚合平台，直接接入虚拟电厂管理云平台并参与电网调节的负荷资源，可接受电网直接调度控制并上报相应的计划申报信息。

### 3.8

#### 负荷聚合商 Load Aggregator

将某一区域中各类用电侧负荷实时运行信息汇集，进行统一管控和运营的单位或者部门。

**注：**聚合方式可以是单一聚合，如容量较大的大工业负荷；也可以多体聚合，如数量众多的分布式小负荷。聚合商可以是社会上各类第三方运营商。

### 3.9

#### 负荷聚合平台 Load Aggregation Platform

为满足可调负荷参与电网调节运行和市场运营业务需求，由负荷聚合商在本地或云端部署的自动化信息系统，具备对各类用电侧负荷资源实时信息接入、实时监控、自动功率控制、市场交易申报、协同指令下达、操作控制、统计查询、计量计费等功能。

### 3.10

#### 虚拟专用网络 Virtual Private Network

一种在公共通信基础网络上通过逻辑方式隔离出来的网络。它是一组封闭的网络，即使通信与开放系统或其他 VPN 共享同一主干网络，其通信也是保持分离的。

### 3.11

#### 虚拟电厂终端 Virtual Power Plant Terminal

一种部署于负荷聚合商或可调节负荷的终端设备，负荷聚合商或可调节负荷可通过虚拟电厂终端接入虚拟电厂管理云平台，实现信息交换。

### 3.12

#### 终端侧安全防护设备 Security Protection Equipment of Terminal Side

以独立硬件设备、嵌入式芯片或软件SDK等形式部署于虚拟电厂终端侧，为业务数据提供数据加密、身份认证等网络安全防护措施。

### 3.13

#### 虚拟电厂数字证书系统 Digital Certificate System of VPP

对虚拟电厂安全防护设备的数字证书进行全生命周期的过程管理，实现证书签发、证书管理、密钥管理等功能。

## 4 缩略语

下列缩略语适用于本文件。

4G 第四代移动通信技术 (4th-Generation)

5G 第五代移动通信技术 (5th-Generation)

SNMP 简单网络管理协议 (Simple Network Management Protocol)

Syslog 系统日志 (System Log)

VPN 虚拟专用网 (Virtual Private Network)

IPSec IP安全协议 (Internet Protocol Security)

SSL 安全套接层 (Secure Socket Layer)

SM1 对称密码算法，使用128比特分组的分组密码算法，用于密钥协商数据的加密保护和报文数据的加密保护

SM2 256比特SM2椭圆曲线密码算法，用于实体验证、数字签名和数字信封等

SM3 密码杂凑算法，用于对称密钥生成和完整性校验，输出为256比特

SM4 对称密码算法，使用128比特分组的分组密码算法，用于密钥协商数据的加密保护和报文数据的加密保护

HMAC 杂凑消息认证码 (Hash Message Authentication Code)

NAT 网络地址转换 (Network Address Transfer)

PKI 公钥基础设施是提供公钥加密和数字签名服务的系统或平台，目的是为了管理密钥和证书 (Public Key Infrastructure)

PKCS12 RSA公司制定的第12个关于非对称密钥的一系列标准 (Public Key Cryptography Standard 12)

## 5 总体目标及要求

### 5.1 总体目标

虚拟电厂终端授信及安全加密的总体目标是抵御黑客、恶意代码等通过各种形式发起的恶意破坏、攻击，以及其它非法操作，防止系统瘫痪和失控，并由此导致的虚拟电厂系统及可调节负荷一次系统事故。

### 5.2 总体要求

5.2.1 应满足国家法律法规和国家技术标准的相关要求，如国家网络安全法、数据安全法、GB/T 22239、GB/T 36572 等。

5.2.2 设备关键组件应实现安全可控，包括核心硬件、操作系统、数据库、密码算法等。

5.2.3 应全面加强设备的通信安全、物理安全、访问控制、入侵防范、数据安全以及过程审计等安全

配置和防护能力。

5.3 网络架构

虚拟电厂终端授信及安全加密的总体网络架构如图1 所示。

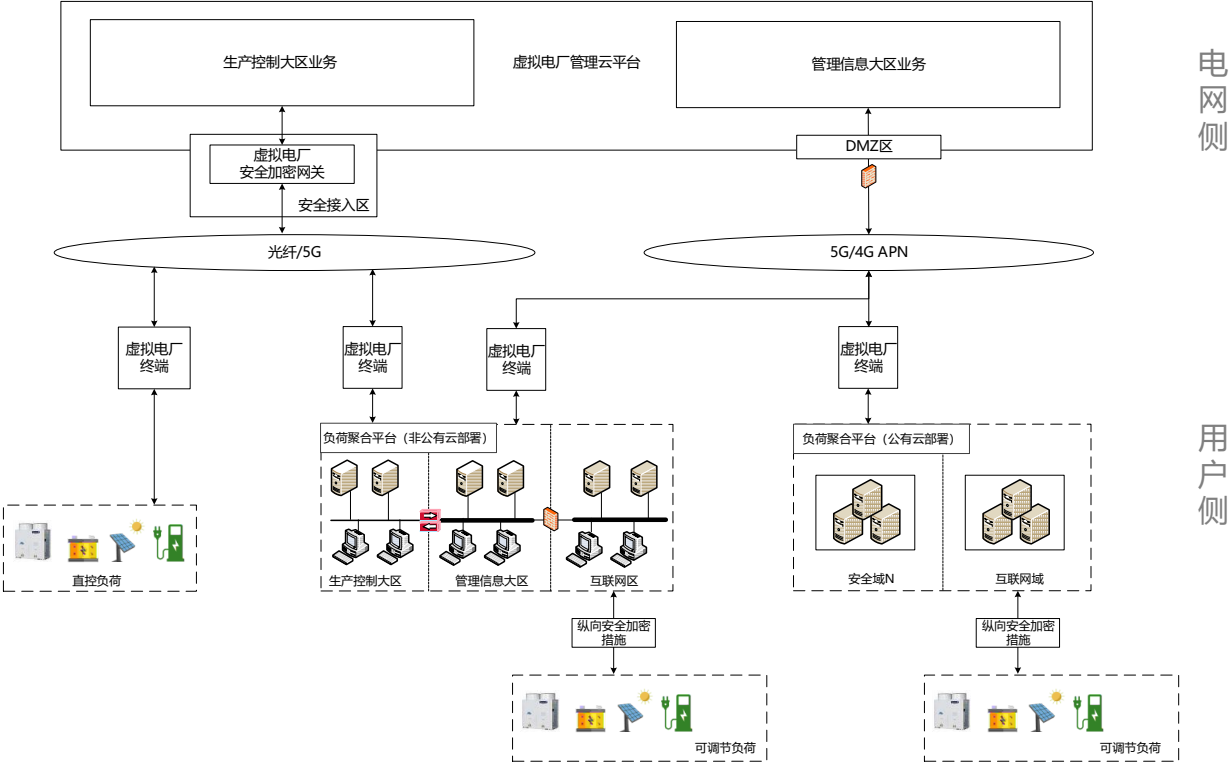


图1 总体网络架构

6 网络安全要求

6.1 安全分区

6.1.1 根据电力监控系统的网络安全要求，参与电网运行的负荷聚合平台应按照业务功能划分相应的安全分区，宜划分为生产控制大区、管理信息大区和互联网区等，当负荷聚合平台包含有实时控制业务模块或未来将建设实时控制功能的业务系统，应划分生产控制大区和管理信息大区。

6.1.2 生产控制大区部署与电网侧实时调控功能相对应的功能模块，涉及负荷聚合平台实时监控与采集、生产控制等相关功能。管理信息大区部署与电网侧管理类功能相对应的功能模块，涉及负荷聚合平台邀约管理，计划申报等相关功能。互联网区用于负荷聚合平台对下与各类可调节负荷连接，完成数据采集与交互相关功能。对于公有云部署的负荷聚合平台应根据功能划分相应的安全区域，不同负荷聚合平台应部署于公有云平台的不同区域。

6.2 网络专用

6.2.1 负荷聚合平台或可调节负荷应通过虚拟电厂终端接入虚拟电厂管理云平台。当接入云平台生产控制大区时应通过光纤、5G 切片网络进行业务数据传输，当接入云平台管理信息大区时应通过 5G 切片、4G APN 等通信网络进行信息交互。

6.2.2 对部分负荷聚合规模较大，其负荷波动可能直接影响电网安全稳定运行的负荷聚合平台，宜进



一步在聚合平台与虚拟电厂终端的边界处部署安全隔离装置，隔离装置须满足 GB/T 37934-2019 的要求。

### 6.3 横向隔离

6.3.1 非公有云部署的负荷聚合平台在生产控制大区和管理信息大区之间应设置经国家指定部门检测认证的电力专用横向单向安全隔离装置，隔离强度应当接近或达到物理隔离，管理信息大区和互联网区之间应采用逻辑隔离措施。

6.3.2 公有云部署的负荷聚合平台不同安全区域之间应采取隔离措施，隔离强度应当接近或达到相应的隔离水平。

### 6.4 纵向认证

6.4.1 通过虚拟电厂终端接入虚拟电厂管理云平台生产控制大区时，应采用国密 IPsec 协议或国密 SSL/TLS 等纵向加密认证措施实现数据传输的加密和身份认证功能。

6.4.2 通过虚拟电厂终端接入虚拟电厂管理云平台管理信息大区时，应采用国密算法进行身份认证、访问控制和数据加密等安全防护措施，确保邀约类业务的安全性。

6.4.3 负荷聚合平台与可调节负荷之间的控制业务交互应采取纵向安全加密措施，加密算法应采用国密加密算法。

### 6.5 终端本体安全

虚拟电厂终端设备应实现自身的安全，应采用安全、可控、可靠的软硬件产品。

### 6.6 操作系统和基础软件安全

操作系统、数据库、中间件等基础软件应防范存在恶意后门，应合理配置、启用安全策略。操作系统和基础软件应仅安装运行需要的组件和应用程序，并及时升级安全补丁，补丁更新前应进行充分的测试。

### 6.7 可信安全免疫

在虚拟电厂终端内部，宜逐步采用基于可信计算的安全免疫防护技术，实现对病毒木马等恶意代码的安全免疫。涉及密码技术的安全设备或防护措施，均采用国产商用密码技术，使用国家商用密码算法（SM1/SM2/SM3/SM4/SM7/SM9 等）。

## 7 安全加密方式

### 7.1 加密实现方式

负荷聚合平台或可调节负荷通过虚拟电厂终端接入虚拟电厂管理云平台，其中安全防护设备的加密实现方式具体分为三种模式：

- a) 外置硬件安全加密装置；
- b) 嵌入式方式集成安全加密芯片；
- c) 采用软件加密 SDK，通过 License 授权方式，提供接口调用方式获取加密算法。

#### 7.1.1 外置硬件安全加密装置

外置硬件安全加密装置的要求如下：

- a) 硬件安全加密装置与虚拟电厂终端的通信接口采用USB或网口；
- b) 应具备密钥存储功能；
- c) 应具备离线、在线更新密钥功能；
- d) 应至少具备两种以上国密加密算法；
- e) 应具备对称加密和非对称加密算法；
- f) 应能存储数字证书；
- g) 应通过国家密码管理局相关检测，并取得国密型号。

### 7.1.2 集成安全加密芯片

集成安全加密芯片模式的要求如下：

- a) 集成安全加密芯片与主主机的通信接口宜采用SPI接口；
- b) 集成安全加密芯片具备离线、在线更新密钥功能；
- c) 应至少具备两种以上国密加密算法；
- d) 应具备对称加密和非对称加密算法；
- e) 应能够存储数字证书；
- f) 安全加密芯片应满足国密二级要求。

### 7.1.3 软件加密 SDK

软件加密SDK模式的要求如下：

- a) 加密SDK应至少具备两种以上国密加密算法；
- b) 应具备对称加密和非对称加密算法；
- c) 应能够安全存储密钥；
- d) 应具备在线更新密钥功能；
- e) 应能够安全存储数字证书。

## 7.2 加解密算法要求

加解密算法要求如下：

- a) 身份认证宜采用国密SM2数字签名算法；
- b) 业务报文加密宜采用国密对称加密算法；
- c) 在线更新密钥时，密钥应加密后进行传输。

## 7.3 通信协议要求

通信协议要求如下：

- a) 对于HTTP业务通信应采用HTTPS协议进行传输加密保护；
- b) 通信通道宜采用TLS、国密IPSec或SSL加密保证传输安全；
- c) 业务数据报文应采用身份认证、加密等安全防护措施进行保护。

# 8 安全加密要求

## 8.1 安全性要求

安全性要求如下：

- a) 依据 GM/T 0022-2014《IPSec VPN 技术规范》或 GM/T 0024-2014《SSL VPN 技术规范》，通过国家密码管理局的鉴定；

b) 依据 GAT 686-2007《虚拟专用网安全技术要求》，获得公安部颁发的 VPN 类型的《计算机信息系统安全专用产品销售许可证》；

c) 能有效防止各类网络攻击，保证设备自身及配电终端安全；

d) 设备密钥应由设备自身产生，其公钥应能被导出。设备密钥应保存在非易失性存储装置中，其私钥应有安全保护措施；

e) 会话密钥产生后应保存在易失性存储器中，达到密钥更新条件后应自动更换，在连接断开、设备断电时应销毁。

## 8.2 功能要求

### 8.2.1 通信加密

通信加密要求如下：

a) 与虚拟电厂管理云平台生产控制大区交互，应支持国密 IPsec 协议或国密 SSL/TLS 等国密 VPN 安全隧道，对业务数据进行加密通信；

b) 与虚拟电厂管理云平台管理信息大区交互，应支持国密算法，对业务数据进行加密和认证安全防护服务。

### 8.2.2 日志管理

终端侧安全防护设备应提供日志记录功能，如系统开机、算法启动自检、随机数启动检测、随机数周期性检测、密钥协商等事件记录日志等，日志的记录及查看由厂家自定义实现。

### 8.2.3 本地配置

终端侧安全防护设备厂商应提供本地配置工具，用于导出证书请求、导入虚拟电厂数字证书系统签发的证书压缩包文件，以及配置终端侧安全防护设备系统参数。

### 8.2.4 远程管理

应具备远程管理功能，接受虚拟电厂安全加密网关的远程管理。

### 8.2.5 自检功能

应具有开机自检功能，能清晰明确地指示故障或状态。

## 8.3 装置稳定性

设备应能承受 GB/T 13729 中 3.9 规定的稳定性试验，装置连续运行 72 小时，每隔 8 小时检测一次。

## 8.4 环境适应性要求

外置硬件安全加密装置的环境适应性要求如下：

a) 环境温度：-40℃ ~ +70℃；

b) 相对湿度：5% ~ 95%，无凝露；

c) 有关正弦稳态振动、冲击、自由跌落的参数等级见 GB/T 15153.2—2000 中第 4 章规定；

d) 装置电源输入通常为 DC 9~48V，并应具备防反接保护，防过流保护功能；

e) 装置在正常运行时，其整体功耗不宜超过 3W。

## 8.5 数字证书签发要求

### 8.5.1 安全性要求

数字证书签发的安全性要求如下：

- a) 依据 GM/T 0014—2012《数字证书认证系统密码协议规范》及其相关安全技术规范，通过国家密码管理局的鉴定；
- b) 应将管理角色和业务操作角色分开，每个角色执行系统的一部分功能，相互独立、相互制约，管理员有独立的安全认证机制，有效保证系统的安全性；
- c) 支持国家密码主管部门批准的算法 SM1、SM2、SM3、SM4；
- d) 采用目前先进成熟的 PKI 密码技术，数字证书的生成、发放、管理以及密钥的生成、管理应当脱离网络，独立运行；
- e) 具有完善的密钥管理功能，保障密钥的生成、存储、使用、更新、废除、归档、销毁、备份和恢复整个生命周期中的安全；
- f) 数字证书系统应具备密钥、策略和证书等本设备运行配置信息的安全备份和还原功能，确保终端侧安全防护设备在紧急故障情况下的业务连续性保障。

### 8.5.2 数字证书系统功能要求

数字证书系统的功能要求如下：

- a) 支持 SM2 双证书（加密证书/签名证书）、双中心（CA 认证中心/密钥管理中心）；
- b) 提供数字证书申请、签发、下载、更新、冻结、解冻、作废等功能，为数字证书提供完善的生命周期管理支持；
- c) 支持 CRL（证书作废列表）的查询及下载，CRL 使用 SM3 算法签名；
- d) 支持多种数字证书模板，用户可以通过证书模板管理功能灵活配置各种算法、用途和格式的数字证书；
- e) 提供事件级审计功能，对涉及系统安全的行为、人员、时间的记录进行跟踪、统计和分析；
- f) 支持系统备份和恢复，确保关键业务数据在发生灾难性破坏时，系统能够及时和尽可能完整的恢复被破坏的数据；
- g) 易于部署与使用，在监控、配置、统计、分析等方面采用可视化的图形界面呈现和操作方式。

### 8.5.3 证书签发接口要求

终端侧安全防护设备正常运行的前提是必须拥有设备密钥及设备证书。本规范中设备证书签发及加密密钥分发工作由虚拟电厂数字证书系统完成。

### 8.5.4 设备证书签发流程

8.5.4.1 由设备厂商负责从终端侧安全防护设备中导出 P10 签名证书请求文件，通过邮件或 U 盘等介质，离线方式发送给虚拟电厂数字证书系统管理员。P10 签名证书请求文件必须包含拥有者（CN），可选包含部门（OU）、组织（O）、城市/地区（L）、省（S）、国家（C）信息。对于虚拟电厂安全加密网关等电网侧安全防护设备，拥有者（CN）应填写网关的工作口 IP；对于终端侧安全防护设备，拥有者（CN）应填写其保护的虚拟电厂终端名称；

8.5.4.2 虚拟电厂数字证书系统生成加密密钥对，并导出对应的证书压缩包文件，该压缩包文件包含根证书、签名证书、加密证书和受保护的加密密钥对，压缩包文件定义参见 8.5.5 小节；

8.5.4.3 设备厂商获取该压缩包文件并导入安全防护设备中，导入方式由设备厂商自行安全地实施。

### 8.5.5 证书文件要求

虚拟电厂数字证书系统导出的证书压缩包文件采用 ZIP 格式，包含下表所示文件。

表1. 证书压缩包文件内容表

文件名	格式	描述
CA.cer	x. 509, der 格式	根证书
sign.cer	x. 509, der 格式	安全防护设备签名证书
enc.cer	x. 509, der 格式	安全防护设备加密证书
encryptedKey	ECC 加密密钥对保护结构	受安全防护设备签名公钥保护的加密密 钥对保护结构文件

## 参 考 文 献

- [1] 国家发改委2014第14号令 电力监控系统安全防护规定
  - [2] 国能安全〔2015〕36号 电力监控系统安全防护总体方案和评估规范
  - [3] 国能发监管规〔2021〕60号 电力并网运行管理规定
-