ICS 43.080
CCS T 47

DB4403

深　圳　市　地　方　标　准

DB4403/T 341—2023

虚拟电厂终端授信及安全加密技术规范

Technical specifications for terminal authentication and security encryption of the virtual power plant

2023-06-12 发布　　2023-07-01 实施

深圳市市场监督管理局　发布

目　　次

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 2
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
参考文献 9

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》的规定起草。

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、北京科东电力控制系统有限责任公司。

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、李曼、车向北、曾诗钦、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、王国栋。

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。

本文件适用于在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，虚拟电厂安全加密终端、数字证书系统及终端侧安全防护设备。

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。

GB/T 13729—2019 远动终端设备

GB/T 20279 信息安全技术 网络和终端隔离产品安全技术要求

GB/T 22239 信息安全技术 网络安全等级保护基本要求

GB/T 36572 电力监控系统网络安全防护导则

GB/T 37934 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

GM/T 0014—2012 数字证书认证系统密码协议规范

GM/T 0022—2014 IPSec VPN技术规范

GM/T 0024—2014 SSL VPN技术规范

3 术语和定义

下列术语和定义适用于本文件。

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

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。

3.3

虚拟电厂 virtual power plant

通过先进通信技术和软件架构，实现地理位置分散的各种分布式负荷的聚合和协调优化，形成虚拟等效的对外功率调节服务，作为一个特殊电厂参与电力市场和电网运行的逻辑实体。

3.4

虚拟电厂管理云平台 virtual power plant management platform

一种基于现有调度控制系统部署的，实现对虚拟电厂统一管理的技术支持系统。

注：是传统调度自动化系统功能的外延拓展，具备实时数据采集、日前计划下发、实时控制及组织市场交易等功能。

3.5

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。

3.6

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。

3.7

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。

3.8

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，

注：具备对各类用电侧负荷资源实时信息接入、实时监视、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。

3.9

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。

3.10

虚拟电厂安全加密终端 virtual power plant security encryption 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安全加密终端接入虚拟电厂管理云平台，实现信息交换。

3.11

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安全加密终端侧，为业务数据提供数据加密、身份认证等网络安全防护措施。

3.12

虚拟电厂数字证书系统 digital certificate system of virtual power plant

对虚拟电厂安全加密终端侧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）
CA：证书授权（Certificate Authority）
CRL：数字证书撤销列表（Certificate Revocation List）
IPSec：IP安全协议（Internet Protocol Security）
OTA：空中下载技术（Over the Air Technology）
PKI：公钥基础设施（Public Key Infrastructure）
PKCS#10：公钥加密标准#10（The Public-Key Cryptography Standards#10）
SSL：安全套接层（Secure Socket Layer）
TLS：传输层安全(Transport Layer Security)
VPN：虚拟专用网（Virtual Private Network）

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GB/T 22239、GB/T 36572、DL/T 2473.2—2022等国家及行业技术标准相关要求。
5.2.2 虚拟电厂终端授信及安全加密相关设备应采用制造和供应链环节无恶意操纵的硬件，应采用经过安全验证且定期更新的操作系统和数据库，应采用密码算法确保敏感数据的存储和传输安全。
5.2.3 虚拟电厂终端授信及安全加密相关设备应具备安全配置和防护能力，包括通信安全、访问控制、入侵防范和数据安全等方面。

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。

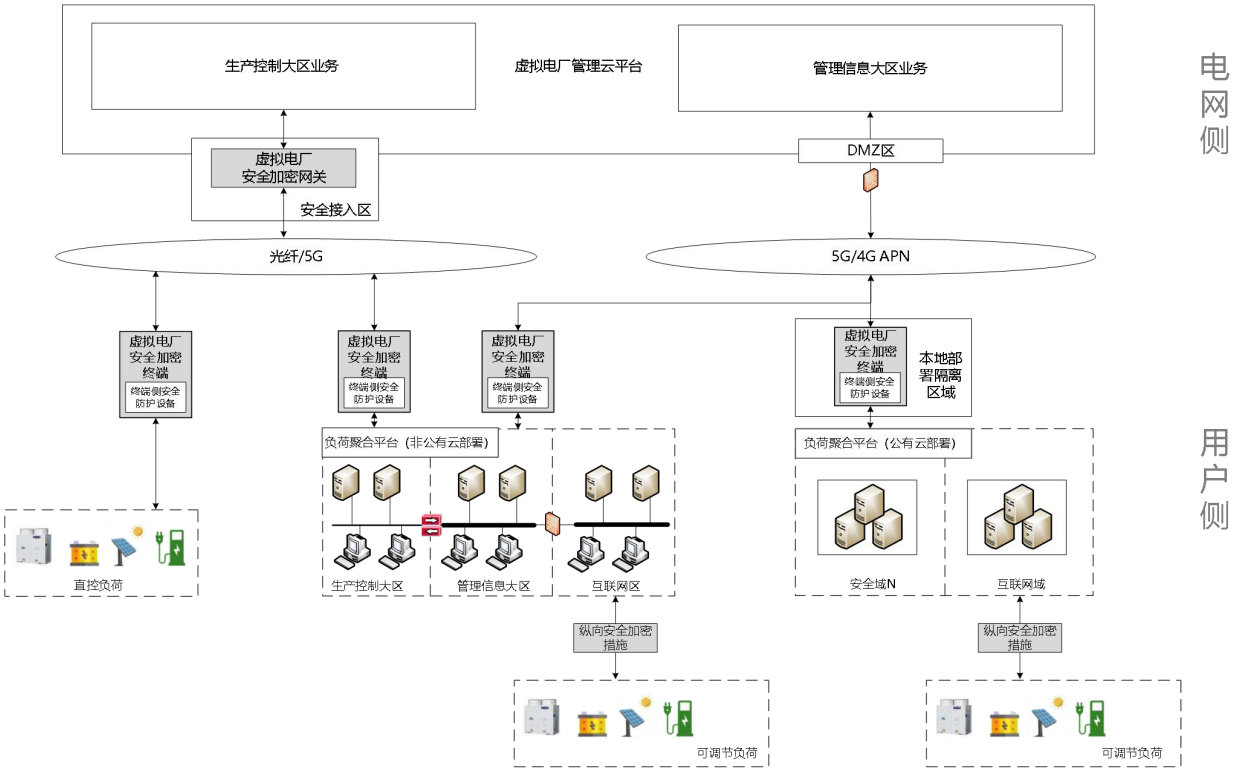

图 1　总体网络架构

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安全加密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安全加密终端的边界处部署安全隔离装置，隔离装置应满足 GB／T 37934 或 GB/T 20279 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　通过虚拟电厂安全加密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　通过虚拟电厂安全加密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

虚拟电厂安全加密终端应实现自身的安全，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

在虚拟电厂安全加密终端内部，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，均应采用国产商用密码技术，使用国家商用密码算法（SM1/SM2/SM3/SM4 等）。

注：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。

7　安全加密方式

7.1　终端侧安全防护设备分类

7.1.1　加密实现方式

负荷聚合平台或可调节负荷通过虚拟电厂安全加密终端接入虚拟电厂管理云平台，其中终端侧安全防护设备的加密实现方式具体分为以下三种模式：

a）　外置硬件安全加密装置；

b）　嵌入式集成安全加密芯片；

c）　采用软件加密 SDK，通过接口调用方式实现安全加密。

7.1.2 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安全加密终端的通信接口可采用 USB、网口、CAN 或 RS 485；
b) 应具备密钥安全存储功能；
c) 应具备离线、在线更新密钥功能；
d) 应具备国密对称加密和国密非对称加密算法；
e) 应能存储数字证书；
f) 应通过国家密码管理局认可检测机构的认证检测，并取得商用密码产品认证证书。

7.1.3 安全加密芯片

安全加密芯片的要求如下：

a) 安全加密芯片的通信接口宜采用 SPI 接口；
b) 应具备密钥安全存储功能；
c) 应具备离线、在线更新密钥功能；
d) 应具备国密对称加密和国密非对称加密算法；
e) 应能够存储数字证书；
f) 应满足国密二级要求；
g) 应具备生成安全真实的随机数；
h) 应具备 Flash 和 RAM 防读取/篡改、芯片防破解。

7.1.4 软件加密 SDK

软件加密SDK的要求如下：

a) 应支持国密算法 SM2、SM3 及 SM4；
b) 应能够安全存储密钥；
c) 应具备更新密钥功能；
d) 应具备国密数字签名功能。

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 SM1 或 SM4 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) 业务数据报文应采用身份认证、加密等安全防护措施进行传输；
c) 对于 OTA 业务通信宜采用国密非对称算法生成的数字签名。

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 或 GM/T 0024—2014；
b) 能有效防止各类网络攻击，保证设备自身及终端安全；
c) 设备密钥应由设备自身产生，其公钥应能被导出，其私钥应有安全保护措施。

8.2 功能要求

8.2.1 日志管理

外置硬件安全加密装置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。

8.2.2 本地配置

终端侧安全防护设备厂商应提供本地配置工具或配置脚本，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。

8.2.3 自检功能

外置硬件安全加密装置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

终端侧安全防护设备应满足 GB/T 13729—2019 中 3.9 的要求，装置连续运行 72 小时。

8.4 数字证书签发要求

8.4.1 安全性要求

虚拟电厂数字证书系统的安全性要求如下：

a) 依据 GM/T 0014—2012 及其相关安全技术规范；
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) 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。

8.4.2 功能要求

虚拟电厂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 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。

8.4.3 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。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。

8.4.4 设备证书签发流程

8.4.4.1 由终端侧安全防护设备厂商负责从设备中导出 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安全加密终端名称。
8.4.4.2 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，证书压缩包文件定义见 8.4.5。
8.4.4.3 设备厂商获取该压缩包文件并导入终端侧安全防护设备中，导入方式由设备厂商自行安全地实施。

8.4.5 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，具体内容如表 1 所示。

表 1 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	终端侧安全防护设备签名证书
enc.cer	x.509,der 格式	终端侧安全防护设备加密证书
encryptedKey	ECC 加密密钥对保护结构	受终端侧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] Q/CSG 212001—2020 中国南方电网电力监控系统安全防护管理办法
[2] Q/CSG 1204009—2015 中国南方电网电力监控系统安全防护技术规范