



中华人民共和国国家标准

GB/T 25320.4—2024

代替 GB/Z 25320.4—2010

电力系统管理及其信息交换 数据和通信安全

第 4 部分：包含 MMS 的协议集及其附件

Power systems management and associated information exchange—
Data and communications security—
Part 4: Profiles including MMS and derivatives

(IEC 62351-4:2018, MOD)

2024-12-31 发布

2025-07-01 实施

国家市场监督管理总局
国家标准化管理委员会 发布

目 次

前言	V
引言	VII
1 范围	1
1.1 概述	1
1.2 代码组件	1
2 规范性引用文件	1
3 术语、定义和缩略语	3
3.1 概述	3
3.2 术语和定义	4
3.3 缩略语	7
4 本文件涉及的安全问题	8
4.1 通信参考模型	8
4.2 应用和传输协议集的安全性	8
4.3 兼容模式和原生模式	9
4.4 应对安全威胁	9
4.5 应对攻击的方法	10
4.6 日志	10
5 具体要求	11
5.1 ICCP/IEC 60870-6-x 通信栈的具体要求	11
5.2 IEC 61850 的具体要求	11
6 传输安全	11
6.1 概述	11
6.2 传输层安全(TLS)的应用	11
6.3 OSI 操作环境中的传输安全	13
6.4 XMPP 操作环境中的通信安全	15
7 应用层安全概述(资料性)	15
7.1 概述	15
7.2 描述技术	16
8 加密算法的应用	17
8.1 概述	17
8.2 基本加密定义	17
8.3 公钥算法	18
8.4 哈希算法	18

8.5	签名算法	18
8.6	对称密钥算法	19
8.7	认证加密算法	19
8.8	完整性校验值算法	20
9	对象标识符分配(规范性)	20
10	通用 OSI 上层需求(规范性)	20
10.1	概述	20
10.2	OSI 上层通用要求	21
10.3	会话层协议要求	21
10.4	表示层协议要求	22
10.5	关联控制服务元素(ACSE)协议要求	24
11	应用安全协议集(规范性)	25
11.1	OSI 针对应用协议集的要求	25
11.2	MMS 认证值	27
12	端到端应用安全模型	28
12.1	简介和总体架构	28
12.2	抽象语法规则	30
13	端到端应用安全(规范性)	30
13.1	关联管理	30
13.2	数据传输阶段	35
13.3	ClearToken 数据类型	36
13.4	身份认证和完整性规范	42
14	端到端安全错误处理(规范性)	43
14.1	概述	43
14.2	诊断规范	43
14.3	端到端安全握手请求和接受检查	46
14.4	数据传输期间安全协议控制信息检查	48
15	OSI 操作环境下的端到端安全	48
15.1	概述	48
15.2	附加的上层需求	49
15.3	OSI 环境下关联管理	49
15.4	OSI 环境下数据传输	52
15.5	OSI 上层路由	52
15.6	OSI 操作环境检查	54
16	XMPP 操作环境中的端到端安全	55
16.1	XMPP 操作环境封装概述	55
16.2	SecPDU 到 iq 节的映射	55

16.3	SecPDU 到 message 节的映射	56
16.4	XMPP 节错误处理	56
16.5	XML 命名空间	57
16.6	XMPP 节中 EnvPDU 的编码	58
16.7	多重关联	58
16.8	释放碰撞考虑	58
17	一致性	58
17.1	通则	58
17.2	符号	58
17.3	操作环境的一致性	59
17.4	操作模式的一致性	59
17.5	兼容模式的一致性	59
17.6	原生模式的一致性	60
附录 A (规范性)	应用安全协议集的 ASN.1 规范	62
附录 B (规范性)	端到端安全的 ASN.1 规范	64
附录 C (规范性)	用于端到端安全的 W3C XSD 规范	72
附录 D (规范性)	OSI 操作环境下的 ASN.1 模型	84
D.1	概要	84
D.2	ASN.1 模型	84
附录 E (规范性)	XMPP 操作环境下的 ASN.1 模型和 W3C 模式文档 XSD	87
E.1	概要	87
E.2	XMPP 操作环境下的 ASN.1 模型	87
E.3	XMPP 操作环境下的 W3C 模式文档 XSD	90
附录 F (规范性)	虚拟 API 规范模板	94
F.1	概要	94
F.2	虚拟 API 对应的 ASN.1 模型	94
F.3	OSI 环境下虚拟 API 对应的 ASN.1 模型	95
F.4	虚拟 API 对应的 W3C 模式文档 XSD	95
附录 G (规范性)	最终实体公钥证书规范	97
G.1	概要	97
G.2	总体要求	97
G.3	长度考虑	97
G.4	基本结构要求及建议	97
G.5	扩展	98
G.6	操作环境的特殊要求	99
附录 H (规范性)	OSI 操作环境下的底层要求	100
H.1	适用范围	100

H.2 传输协议 TP0	100
H.3 IETF RFC 1006	101
附录 I (资料性) ACSE 的 ASN.1 定义	102
参考文献	108
图 1 应用和传输协议集(资料性)	8
图 2 含有或不含 TLS 保护的传输配置	13
图 3 建立连接	21
图 4 在会话层数据传输 SPDU 中包含用户数据	23
图 5 端到端安全构建块	29
图 6 环境、端到端安全与受保护协议之间的关系	29
图 7 APDUs 之间的关系	29
图 8 端到端安全规范的范围	30
图 9 上层路由	53
图 F.1 虚拟 API 概念	94
表 1 安全和安全措施组合之间的关系	9
表 2 GB/Z 25320.4—2010 推荐密码套件	14
表 3 本文件文中的密码套件组合	15
表 4 SecPDUs 和 ACSE APDUs 之间映射	49
表 5 SecPDU 到 XMPP 节的映射	55
表 6 操作环境的一致性	59
表 7 操作模式的一致性	59
表 8 兼容模式下 TLS 密码套件的一致性	60
表 9 加密模式的一致性	60
表 10 原生模式下 TLS 密码套件的一致性	60
表 11 E2E 安全加密算法的一致性	61
表 H.1 传输协议 TP0 各种 TPDU 最大帧长	100

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。

本文件是 GB/T(Z) 25320《电力系统管理及其信息交换 数据和通信安全》的第 4 部分。GB/T(Z) 25320 已经发布了以下部分：

- 第 1 部分：通信网络和系统安全 安全问题介绍；
- 第 2 部分：术语；
- 第 3 部分：通信网络和系统安全 包含 TCP/IP 的协议集；
- 第 4 部分：包含 MMS 的协议集及其附件；
- 第 5 部分：GB/T 18657 等及其衍生标准的安全；
- 第 6 部分：IEC 61850 的安全；
- 第 7 部分：网络和系统管理(NSM)的数据对象模型；
- 第 11 部分：XML 文件的安全；
- 第 100-1 部分：IEC TS 62351-5 和 IEC TS 60870-5-7 的一致性测试用例；
- 第 100-3 部分：IEC 62351-3 的一致性测试用例和包括 TCP/IP 协议集的安全通信扩展。

本文件代替 GB/Z 25320.4—2010《电力系统管理及其信息交换 数据和通信安全 第 4 部分：包含 MMS 的协议集》，与 GB/Z 25320.4—2010 相比，除结构调整和编辑性改动外，主要技术变化如下：

- a) 更改了适用范围(见第 1 章,2010 年版的第 1 章)；
- b) 更改了术语和定义,增加了缩略语(见第 3 章,2010 年版的第 3 章)；
- c) 更改了本文件涉及的安全问题(见第 4 章,见 2010 年版的第 4 章)；
- d) 删除了应用协议集(A-Profile)安全(见 2010 年版的第 5 章)；
- e) 删除了传输协议集(T-Profile)安全(见 2010 年版的第 6 章)；
- f) 增加了具体要求(见第 5 章)；
- g) 增加了传输安全(见第 6 章)；
- h) 增加了应用层安全概述(见第 7 章)；
- i) 增加了加密算法的应用(见第 8 章)；
- j) 增加了对象标识符分配(见第 9 章)；
- k) 增加了通用 OSI 上层需求(见第 10 章)；
- l) 增加了端到端应用安全模型(见第 12 章)；
- m) 增加了端到端应用安全(见第 13 章)；
- n) 增加了端到端安全错误处理(见第 14 章)；
- o) 增加了 OSI 操作环境下的端到端安全(见第 15 章)；
- p) 增加了 XMPP 操作环境中的 E2E 安全(见第 16 章)；
- q) 更改了一致性(见第 17 章,见 2010 年版的第 7 章)；
- r) 增加了应用安全协议集的 ANS.1 规范(见附录 A)；
- s) 增加了端到端安全的 ANS.1 规范(见附录 B)；
- t) 增加了用于端到端安全的 W3C XSD 规范(见附录 C)；
- u) 增加了 OSI 操作环境下的 ANS.1 模型(见附录 D)；
- v) 增加了 XMPP 操作环境下的 ANS.1 模型和 W3C 模式文档 XSD(见附录 E)；

- w) 增加了虚拟 API 模板规范(见附录 F);
- x) 增加了最终实体公钥证书规范(见附录 G);
- y) 增加了 OSI 操作环境下的底层要求(见附录 H)。

本文件修改采用 IEC 62351-4:2018《电力系统管理及其信息交换 数据和通信安全 第 4 部分:包含 MMS 的协议集及其附件》。

本文件与 IEC 62351-4:2018 的技术差异及其原因如下:

——规范性引用文件 IEC 62351-3、IEC TS 62351-8、IEC 62351-9、ISO 8601-1 更新至最新版本。

请注意本文件的某些内容可能涉及专利。本文件的发布机构不承担识别专利的责任。

本文件由中国电力企业联合会提出。

本文件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。

本文件起草单位:中国电力科学研究院有限公司、国家电网有限公司国家电力调度控制中心、中国南方电网有限公司、国网上海市电力公司、国网天津市电力有限公司、广东电网有限责任公司电力调度控制中心、国网电力科学研究院有限公司、南京南瑞继保工程技术有限公司、东方电子股份有限公司、国电南瑞南京控制系统有限公司、许继电气股份有限公司、国电南京自动化股份有限公司、长园深瑞继保自动化有限公司、积成电子股份有限公司、北京四方继保工程技术有限公司、国电南瑞科技股份有限公司、上海宽域工业网络设备有限公司。

本文件主要起草人:张金虎、纪欣、张晓、苏扬、王治华、吴金宇、高翔、卢建刚、赵瑞锋、孙丹、张小飞、李广华、温树峰、盛福、贾德顺、万首丰、刘文彪、徐浩、孙发恩、沈艳、许艾、李洪池、南祎、汤方剑、王珍珍、安泰、张丹、张良、肖涛。

本文件及其所代替文件的历次版本发布情况为:

——2010 年首次发布为 GB/Z 25320.4—2010;

——本次为第一次修订。

引 言

GB/T(Z) 25320《电力系统管理及其信息交换 数据和通信安全》，旨在尽可能地减少通信和计算机网络中存在的恶意攻击对电力系统的数据及通信安全产生的危害，完善电力系统使用的各层通信协议中的安全漏洞以及提高电力系统信息基础设施的安全管理。拟由以下部分构成。

- 第 1 部分:通信网络和系统安全 安全问题介绍。目的在于介绍 GB/T(Z) 25320 的其他部分,主要向读者介绍应用于电力系统运行的信息安全的各方面知识。
- 第 2 部分:术语。目的在于介绍在 GB/T 25320(Z)中所使用的关键术语。
- 第 3 部分:通信网络和系统安全 包含 TCP/IP 的协议集。目的在于规定如何通过限于传输层安全协议的消息、过程和算法的规范,对基于 TCP/IP 的协议进行安全防护,使这些协议能适用于 IEC TC 57 的远动环境。
- 第 4 部分:包含 MMS 的协议集及其附件。目的在于规定了对基于 GB/T 16720(ISO 9506)制造报文规范(MMS)及其衍生标准的应用进行安全防护的过程、协议扩充和算法。
- 第 5 部分:GB/T 18657 等及其衍生标准的安全。目的在于定义了应用配置文件(a-profile)安全通信机制,规定了对基于或衍生于 IEC 60870-5(GB/T 18657《远动设备及系统 第 5 部分:传输规约》)的所有协议的运行进行安全防护的消息、过程和算法。
- 第 6 部分:IEC 61850 的安全。目的在于规定了对基于或派生于 IEC 61850 的所有协议的运行进行安全防护的报文、过程与算法。
- 第 7 部分:网络和系统管理(NSM)的数据对象模型。目的在于定义了电力系统运行所特有的网络和系统管理的数据对象模型。
- 第 8 部分:基于角色的访问控制。目的在于为电力系统管理提供基于角色的访问控制。
- 第 9 部分:电力系统设备的网络安全密钥管理。目的在于通过指定或限制要使用的密钥管理选项来定义实现密钥管理互操作性的要求和技术。
- 第 10 部分:安全架构指南。目的在于描述基于基本安全控制的电力系统安全架构指南。
- 第 11 部分:XML 文件的安全。目的在于规范智能变电站通信过程中的配置文件(XML 文件)的安全性。
- 第 12 部分:分布式能源(DER)系统的快速恢复和安全建议。目的在于提高分布式能源(DER)系统的安全性和可靠性。
- 第 13 部分:标准和规范中涉及的安全主题指南。目的在于提供关于电力行业使用的标准和规范(IEC 或其他)中可能或应该涵盖哪些安全问题。
- 第 90-1 部分:电力系统中基于角色的访问控制处理指南。目的在于开发用于定义和设计自定义角色以及角色映射的标准化方法。
- 第 90-2 部分:加密通信的深度包检测。目的在于说明应用于 IEC 62351 保护的通信信道的 DPI 最新技术。
- 第 90-3 部分:网络和系统管理指南。目的是提供处理 IT 和 OT 数据的导则。
- 第 100-1 部分:IEC TS 62351-5 和 IEC TS 60870-5-7 的一致性测试用例。目的在于提供了 IEC 62351-5:2023 和 IEC TS 60870-5-7:2013 的一致性和/或互操作性测试的测试用例。
- 第 100-3 部分:IEC 62351-3 的一致性测试用例和包括 TCP/IP 协议集的安全通信扩展。目的在于提供了 IEC 62351-3:2023 一致性测试用例及验证影响安全扩展程序和协议行为的所有参数的配置。

——第 100-6 部分:IEC 61850-8-1 和 IEC 61850-9-2 的网络安全一致性测试。目的在于提供了变电站自动化系统和远动系统的数据和通信安全互操作性一致性测试的测试用例。

GB/T(Z) 25320《电力系统管理及其信息交换 数据和通信安全》定义了电力系统相关通信协议(IEC 60870-5、IEC 60870-6、IEC 61850、IEC 61970 和 IEC 61968 系列)的数据和通信安全,也定义了通信过程中可能遭受到的安全威胁和安全攻击以及安全应对措施。

本文件是 GB/T(Z) 25320《电力系统管理及其信息交换 数据和通信安全》的第 4 部分,对基于 GB/T 16720(ISO 9506)制造报文规范(MMS)及其衍生标准的应用进行安全防护的过程、协议扩充和算法。

电力系统管理及其信息交换

数据和通信安全

第 4 部分:包含 MMS 的协议集及其附件

1 范围

1.1 概述

本文件扩展了 GB/Z 25320.4—2010[1]¹⁾ 的范围,规定了一种兼容模式——该模式提供了与基于 GB/Z 25320.4—2010 的实现之间的互操作性,并规定了称为原生模式的扩展功能。

本文件阐明了传输层和应用层的安全要求。GB/Z 25320.4—2010 主要在应用层为基于制造消息规范(MMS)的应用在握手期间的认证提供了一些有限的支持,本文件还为握手阶段和数据传输阶段提供了对扩展完整性和认证的支持,在应用层提供了共享密钥管理和数据传输加密,并提供零个或多个中间实体的端到端安全(E2E)。GB/Z 25320.4—2010 仅支持基于 MMS 的系统,即使用开放系统互操作(OSI)协议栈的系统,本文件还支持使用其他协议栈的应用协议,例如互联网协议套件(见 4.1)。该支持扩展到保护使用 XML 编码的应用协议。应用层的这种扩展安全性称为 E2E 安全性。

除了 E2E 安全性之外,本文件还提供了携带安全相关信息的环境协议的映射方式。目前只考虑 OSI 和 XMPP 环境。

本文件作为需要以安全方式使用应用协议(例如 MMS)的标准来规范性引用。

预计存在基于 GB/Z 25320.4—2010 传输安全协议集和应用安全协议集规范的实现,特别是控制中心间通信协议(ICCP)实现。因此,本文件包含了 GB/Z 25320.4—2010 的规范。支持这些规范的实现将与基于 GB/Z 25320.4—2010 的实现相互配合。

注:从严格意义上说,应用安全协议集并不是一个协议栈,但出于历史原因,该术语在此保留。

本文件定义了一组用于保护应用协议的强制性和可选的安全规范。

本文件的最初使用者是制定或使用协议的工作组成员。为了使本文件所述措施生效,协议规范应接受并引用这些措施。

本文件的后续使用者是实现这些协议的产品开发人员,以及希望为自己的环境指定需求的最终用户。

为了理解工作的目的和要求,本文件的部分内容也可能对管理人员和执行人员适用。

1.2 代码组件

购买 IEC 文件时,买方可根据 IEC 软件许可条件,直接或通过分销商向最终用户出售包含本文件代码组件的软件,该许可可在以下网址找到:www.iec.ch/CCv1。

IEC 文件中包含的代码组件也可作为电子阅读器可读文件,网址为 www.iec.ch/public/tc57/supportdocuments/IEC_62351-4.ASN_1.XSD.full.zip。

本文件中的代码组件包含在附录 A、附录 B、附录 C、附录 D 和附录 E 中。

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

1) 方括号内的数字指参考文献。