ICS 29.240.01
CCS F 21

中华人民共和国国家标准

GB/T 25320.11—2023/IEC 62351-11:2016

电力系统管理及其信息交换 数据和通信安全 第11部分:XML文件的安全

Power systems management and associated information exchange—Data and communications security—Part 11: Security for XML documents

(IEC 62351-11:2016,IDT)

2023-12-28 发布　　2024-07-01 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

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11部分。GB/T 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　包括TCP/IP的协议集;

——第4部分:包含MMS的协议集;

——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。

本文件等同采用IEC 62351-11:2016《电力系统管理及其信息交换　数据和通信安全　第11部分:XML文件的安全》。

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:国网电力科学研究院有限公司、国电南瑞能源有限公司、南京南瑞继保电气有限公司、中国电力科学研究院有限公司、国网智能电网研究院有限公司、东南大学、国电南京自动化股份有限公司、中国南方电网电力调度控制中心、国网上海市电力公司、江苏宏源电气有限责任公司、国网吉林省电力有限公司。

本文件主要起草人:孙丹、郭王勇、张丹、温树峰、孔红磊、王珍珍、李广华、姬广龙、袁莉、王宇、王甜甜、窦仁晖、张涛、石卫军、吴在军、陈新之、窦晓波、费稼轩、张小飞、朱鑫泉、陶文伟、王治华、李响、徐洪海、刘昌旭、杨松。

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》,旨在尽可能的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(Z) 25320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。目的在于规定了对基于GB/T 16720(ISO 9506)制造报文规范(MMS)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程序配置文件(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 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。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。

电力系统管理及其信息交换 数据和通信安全 第11部分:XML文件的安全

1 范围

本文件规定了用于保护IEC范围内使用的XML文件以及其他领域(例如IEEE、专利等)中文件的格式、过程和算法。如果需要安全交换,则本文件旨在被标准引用,除非各方之间达成协议以使用其他公认的安全交换机制。

本文件使用了W3C标准来实现XML文件安全性,并提供了这些标准以及其他扩展的介绍。本文件为扩展部分提供了如下规定。

——Header(信息头):Header包含已创建保存文件的相关信息,例如创建IEC 62351-11的XML文件的日期和时间。

——可选择以加密或非加密格式来封装原始XML文件。如果选择加密,则会提供一种机制来表示以可互操作的方式执行加密所需的信息。

——AccessControl(访问控制):表示与原始XML文件中包含的信息有关的访问控制信息的机制。

——Body(正文):用于包含要封装的原始XML文件。

——Signature(签名):能用于身份验证和篡改检测的签名。

总体结构应符合图1。

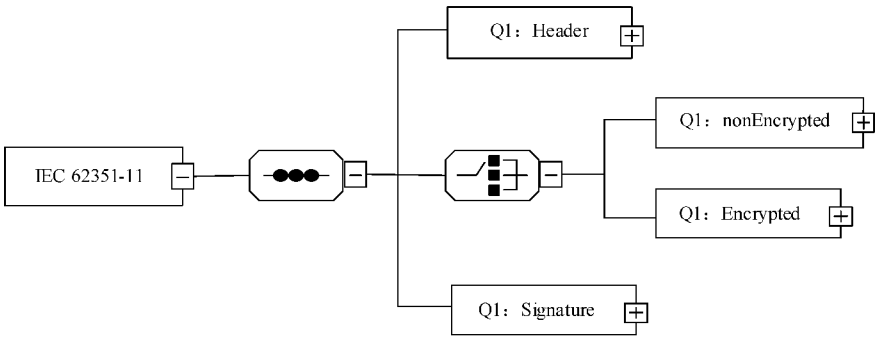

图1 IEC 62351-11的XML文件结构概述

为使本文件中所述的方法生效,需被规范接受和引用。编写本文件是为了启用该流程。

本文件的读者是实现这些规范的产品开发人员。

本文件的部分内容也可供管理人员和执行人员使用,以了解工作的目的和要求。

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。

IEC TS 62351-2 电力系统管理及其信息交换 数据和通信安全 第2部分:术语(Power sys-