Chinastandards.org

ICS 29.240.01
CCS F 21

NATIONAL STANDARD OF THE PEOPLE'S REPUBLIC OF CHINA

GB/T 25320.11-2023

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

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

(English Translation)

Issued on: December 28, 2023 **Implemented on: July 1, 2024**

Issued by: State Administration for Market Regulation, China National Standardization Administration

Preview: page 1 of 5 shown, 29 in the full document. Complete English PDF, instant download:
https://chinastandards.org/standards/gb-t-25320-11-2023

Chinastandards.org

Table of Contents

Preface
Introduction
1 Scope
2 Normative references
3 Terms and Definitions
4 Security issues covered by this document
4.1 Overview
4.2 Responding to security threats
4.3 Dealing with security attacks
5 XML files
6 XML file encapsulation
6.1 Overview
6.2 Information header type HeaderType
6.3 Information
6.4 Encrypted
6.5 SignatureTypeSignatureType
6.6 Supported XSD types
6.7 Security algorithm selection
7 Sample files (informative)
7.1 Non-encrypted example
7.2 Encryption Example
8 IANA signature, digest and encryption method list (informative)
Reference

Foreword

This document complies with the provisions of GB/T 1.1-2020 "Standardization Work Guidelines Part 1: Structure and Drafting Rules of Standardization Documents" Drafting:

This document is Part 11 of GB/T (Z) 25320 "Power System Management and Information Exchange Data and Communication Security": GB/T 25320 the following sections have been published:

---Part 1: Introduction to communication network and system security issues;

Preview: page 2 of 5 shown, 29 in the full document. Complete English PDF, instant download:
https://chinastandards.org/standards/gb-t-25320-11-2023

---Part 2: Terminology;

---Part 3: Communication network and system security including TCP/IP protocol set;

---Part 4: Protocol set including MMS;

---Part 5: Safety of GB/T 18657 and other standards and their derivatives;

---Part 6: Safety of IEC 61850;

---Part 7: Data Object Model for Network and System Management (NSM);

---Part 11: Security of XML files;

---Part 100-1: Conformance test cases for IEC TS62351-5 and IEC TS60870-5-7;

---Part 100-3: Conformance test cases for IEC 62351-3 and secure communication extensions including the TCP/IP protocol set:

This document is equivalent to IEC 62351-11:2016 "Power system management and its information exchange data and communication security Part 11:

Security of XML Files":

Certain contents of this document may be covered by patents: The publisher of this document assumes no responsibility for identifying patents:

Introduction

GB/T (Z) 25320 "Power System Management and Information Exchange Data and Communication Security", which aims to reduce communication and computing as much as possible in order to avoid the harm caused by malicious attacks in the computer network to the data and communication security of the power system, it is necessary to improve the communication protocols at all levels used in the power system:

discuss security vulnerabilities and improve the security management of power system information infrastructure: It is planned to consist of the following parts:

---Part 1: Introduction to communication network and system security issues: The purpose is to introduce other parts of GB/T (Z)25320 it mainly introduces readers to all aspects of information security applied to power system operation:

---Part 2: Terminology: The purpose is to introduce the key terms used in GB/T (Z) 25320:

---Part 3: Communication Network and System Security includes the TCP/IP protocol set: The purpose is to specify how transmission is limited to specifications of the messages, processes and algorithms of layer security protocols, and provide security protection for TCP/IP-based protocols so that these protocols can Suitable for IEC TC57 telecontrol environment:

Preview: page 3 of 5 shown, 29 in the full document. Complete English PDF, instant download:
https://chinastandards.org/standards/gb-t-25320-11-2023

---Part 4: Contains the protocol set of MMS: The purpose is to stipulate the manufacturing message specifications based on GB/T 16720 (ISO 9506) the process, protocol extensions and algorithms for security protection of MMS applications:

---Part 5: Security of GB/T 18657 and other standards and their derivatives: The purpose is to define the application configuration file (a-profile) Secure communication mechanism that specifies the secure operation of all protocols based on or derived from IEC 60870-5 Protected messages, processes and algorithms:

---Part 6: Safety of IEC 61850: The purpose is to specify the operation of all protocols based on or derived from IEC 61850:

Messages, processes and algorithms for security protection:

---Part 7: Data Object Model for Network and System Management (NSM): The purpose is to define the characteristics unique to power system operation:

A data object model for network and systems management:

---Part 8: Role-based access control: The purpose is to provide role-based access control for power system management:

---Part 9: Network security key management of power system equipment: The purpose is to manage by specifying or restricting the keys to be used Options to define requirements and technologies for achieving key management interoperability:

---Part 10: Security Architecture Guidelines: The purpose is to describe guidelines for a power system security architecture based on basic security controls:

---Part 11: Security of XML files: The purpose is to standardize the configuration file (XML file) in the communication process of smart substations security:

---Part 12: Rapid recovery and security recommendations for distributed energy resources (DER) systems: The aim is to improve distributed energy (DER) system security and reliability:

---Part 13: Guidance on safety topics covered in standards and specifications: The purpose is to provide standards and regulations for use in the power industry What safety issues could or should be covered in the specification (IEC or other):

---Part 90-1: Guidelines for handling role-based access control in power systems: The purpose is to develop custom A standardized approach to defining roles and role mapping:

---Part 90-2: Deep packet inspection of encrypted communications: The purpose is to describe the methods applied to communication channels protected by IEC 62351 DPI latest technology:

---Part 90-3: Network and System Administration Guide: The purpose is to provide guidelines for handling IT and OT data:

Preview: page 4 of 5 shown, 29 in the full document. Complete English PDF, instant download:
https://chinastandards.org/standards/gb-t-25320-11-2023

---Part 100-1: Conformance test cases for IEC 62351-5 and IEC TS60870-5-7: The purpose is to provide Test cases for conformance and/or interoperability testing of IEC 62351-5:2023 and IEC TS60870-5-7:2013:

---Part 100-3: Conformance test cases for IEC 62351-3 and secure communication extensions including the TCP/IP protocol set: Purpose it provides IEC 62351-3:2023 conformance test cases and verifies all aspects that affect security extensions and protocol behavior:

Configuration of parameters:

---Part 100-6: Network security conformance testing of IEC 61850-8-1 and IEC 61850-9-2: The purpose is to provide changes Test cases for conformance testing of data and communication security interoperability of power plant automation systems and telecontrol systems:

GB/T (Z) 25320 "Power System Management and Information Exchange Data and Communication Security" defines power system-related communication protocols (IEC 60870-5, IEC 60870-6, IEC 61850, IEC 61970 and IEC 61968 series) data and communication security: defines the pass Security threats and security attacks that may be encountered during the communication process, as well as security countermeasures:

Power system management and information exchange Data and communications security Part 11: Security of XML files

1 Scope

This document specifies methods for protecting XML files used within the scope of IEC as well as files in other fields (e.g. IEEE, patents, etc:) Format, process and algorithm: If secure exchange is required, this document is intended to be referenced by the standard, unless there is agreement between the parties to use another Recognized secure exchange mechanism:

This document uses W3C standards for XML file security and provides an introduction to these standards and other extensions: This article the software provides the following provisions for extensions:

---Header (information header): Header contains relevant information about the created saved file, such as creating the XML of IEC 62351-11 the date and time of the file:

---You can choose to encapsulate the original XML file in encrypted or non-encrypted format: If encryption is selected, a mechanism is provided to represent Represents the information required to perform encryption in an interoperable manner:

---AccessControl: A mechanism that represents access control information related to the information contained in the original XML file:

Preview: page 5 of 5 shown, 29 in the full document. Complete English PDF, instant download:
https://chinastandards.org/standards/gb-t-25320-11-2023