Chinastandards.org

ICS 29.240.30
CCS F 21

NATIONAL STANDARD OF THE

PEOPLE'S REPUBLIC OF CHINA

GB/T 25320.4-2024

Replacing GB/Z 25320.4-2010

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

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

(English Translation)

Issued on: December 31, 2024 **Implemented on: July 1, 2025**

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

Preview: page 1 of 5 shown, 108 in the full document. Complete English PDF, instant download:
https://chinastandards.org/standards/gb-t-25320-4-2024

Chinastandards.org

Table of Contents

Preface
Introduction
1 Scope
1.1 Overview
1.2 Code Components
2 Normative references
3 Terms, definitions and abbreviations
3.1 Overview
3.2 Terms and Definitions
3.3 Abbreviations
4 Security issues covered by this document
4.1 Communication Reference Model
4.2 Security of application and transport protocol suites
4.3 Compatibility Mode and Native Mode
4.4 Responding to Security Threats
4.5 Methods to deal with attacks
4.6 Log
5 Specific requirements
5.1 Specific requirements of ICCP/IEC 60870-6-x communication stack
5.2 Specific requirements of IEC 61850
6 Transmission Security
6.1 Overview
6.2 Application of Transport Layer Security (TLS)
6.3 Transport Security in the OSI Operating Environment
6.4 Communication security in the XMPP operating environment
7 Application Layer Security Overview (Informative)
7.1 Overview
7.2 Description Techniques
8 Application of encryption algorithm
8.1 Overview
8.2 Basic encryption definition
8.3 Public Key Algorithm

Preview: page 2 of 5 shown, 108 in the full document. Complete English PDF, instant download:
https://chinastandards.org/standards/gb-t-25320-4-2024

Chinastandards.org

8.4 Hash Algorithms
8.5 Signature Algorithm
8.6 Symmetric Key Algorithms
8.7 Authenticated Encryption Algorithm
8.8 Integrity Check Value Algorithm
9 Object Identifier Allocation (Normative)
10 General OSI upper layer requirements (normative)
10.1 Overview
10.2 OSI upper layer common requirements
10.3 Session Layer Protocol Requirements
10.4 Presentation Layer Protocol Requirements
10.5 Association Control Service Element (ACSE) Protocol Requirements
11 Application Security Protocol Set (Normative)
11.1 OSI Requirements for Application Protocol Suite
11.2 MMS authentication value
12 End-to-end application security model
12.1 Introduction and overall architecture
12.2 Abstract Syntax Specification
13 End-to-end application security (normative)
13.1 Association Management
13.2 Data transmission phase
13.3 ClearToken Data Type
13.4 Identity Authentication and Integrity Specifications
14 End-to-end secure error handling (normative)
14.1 Overview
14.2 Diagnostic criteria
14.3 End-to-end security handshake request and acceptance checks
14.4 Security protocol control information inspection during data transmission
15 End-to-end security in the OSI operating environment
15.1 Overview
15.2 Additional upper-level requirements
15.3 Association Management in the OSI Environment
15.4 Data Transmission in an OSI Environment
15.5 OSI Upper Layer Routing
15.6 OSI Operational Environment Check

Preview: page 3 of 5 shown, 108 in the full document. Complete English PDF, instant download:
https://chinastandards.org/standards/gb-t-25320-4-2024

Chinastandards.org

16 End-to-end security in the XMPP operating environment
16.1 Overview of XMPP Operating Environment Packaging
16.2 Mapping of SecPDU to iq Section
16.3 Mapping of SecPDU to message section
16.4 XMPP Stanza Error Handling
16.5 XML Namespaces
16.6 Encoding of EnvPDU in XMPP Section
16.7 Multiple Associations
16.8 Release Collision Considerations
17 Consistency
17.1 General
17.2 Symbols
17.3 Consistency of the operating environment
17.4 Consistency of operating modes
17.5 Compatibility Mode Consistency
17.6 Native Mode Consistency
Appendix A (Normative) ASN.1 Specification for the Application Security Protocol Suite
Appendix B (Normative) ASN.1 Specification for End-to-End Security
Appendix C (Normative) W3C XSD Specification for End-to-End Security
Appendix D (Normative) ASN.1 Model in the OSI Operating Environment
D.1 Overview
D.2 ASN.1 Model
Appendix E (Normative) ASN.1 Model and W3C Schema Document XSD 87 for XMPP Operation Environment
E.1 Overview
E.2 ASN.1 model in the XMPP operating environment

Foreword

This document is in accordance with the provisions of GB/T 1.1-2020 "Guidelines for standardization work Part 1: Structure and drafting rules for standardization documents" Drafting.

This document is Part 4 of GB/T (Z) 25320 "Power system management and information exchange data and communication security".

GB/T (Z) 25320 has published the following parts.

Preview: page 4 of 5 shown, 108 in the full document. Complete English PDF, instant download:
https://chinastandards.org/standards/gb-t-25320-4-2024

Chinastandards.org

--- Part 1: Introduction to security issues of communication networks and systems;

--- Part 2: Terminology;

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

--- Part 4: Contains the MMS protocol set and its annexes;

--- Part 5: Safety of GB/T 18657 and its derivative standards;

--- Part 6: Safety of IEC 61850;

--- Part 7: Data object model for network and system management (NSM);

--- Part 11: Security of XML documents;

--- 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 security communications extensions including the TCP/IP protocol suite.

This document replaces GB/Z 25320.4-2010 "Power system management and information exchange data and communication security Part 4: Packet Compared with GB/Z 25320.4-2010, in addition to structural adjustments and editorial changes, the main technical changes are as follows.

a) The scope of application has been changed (see Chapter 1, Chapter 1 of the 2010 edition);

b) The terms and definitions have been changed and abbreviations have been added (see Chapter 3, Chapter 3 of the 2010 edition);

c) The safety issues involved in this document have been changed (see Chapter 4, see Chapter 4 of the 2010 edition);

d) Application Protocol Profile (A-Profile) security has been deleted (see Chapter 5 of the 2010 edition);

e) Deleted the Transport Protocol Suite (T-Profile) security (see Chapter 6 of the 2010 edition);

f) Added specific requirements (see Chapter 5);

g) increased transmission security (see Chapter 6);

h) Added an overview of application layer security (see Chapter 7);

i) Added the application of encryption algorithm (see Chapter 8);

j) Added object identifier allocation (see Chapter 9);

k) Added general OSI upper layer requirements (see Chapter 10);

Preview: page 5 of 5 shown, 108 in the full document. Complete English PDF, instant download:
https://chinastandards.org/standards/gb-t-25320-4-2024