Chinastandards.org

ICS 35.030
CCS L 80

GM

GM/T 0119-2022

Cryptography applications technical specificationfor PLC system and PLC controller

PLC控制系统及PLC控制器密码应用技术规范

(English Translation)

Issued on: November 20, 2022 **Implemented on: June 1, 2023**

Issued by: State Administration of Cryptography

Preview: page 1 of 5 shown, 118 in the full document. Complete English PDF, instant download:
https://chinastandards.org/standards/gm-t-0119-2022

Chinastandards.org

Table of Contents

Requirements for the Cryptography Application of Security Management Server 36 1

11 Requirements for the Cryptography Application of Security Management Server 36

12 Cryptography Application Interface of the PLC System... 36 Appendix A (Informative) Components of PLC System... 38 Appendix B (Informative) Cryptography Security Management Interface Reference 41 Appendix C (Informative) Reference of Cryptography Security Service Interface.. 118 Cryptography Applications Technical Specification for PLC System and PLC Controller

1 Scope

This Document describes the basic components of PLC systems and PLC controllers; defines the cryptography application function of PLC systems, the overall requirements for cryptography application of PLC systems, and the basic process of cryptography application;

defines the cryptography application function and cryptography application requirements of each component device in the PLC system; and provides a reference for the cryptography application interface of the PLC system.

This Document is applicable to the design and development of PLC systems and PLC controllers with integrated cryptography functions; and can also be used to guide the cryptography application detection of related products.

2 Normative References the provisions in following documents become the essential provisions of this Document through reference in this Document. For the dated documents, only the versions with the dates indicated are applicable to this Document; for the undated documents, only the latest version (including all the amendments) is applicable to this Document.

GB/T 32905 Information security techniques - SM3 cryptographic hash algorithm GB/T 32907 Information security techno1ogy - SM4 block cipher algorithm GB/T 32918 (all parts) Information security technology - Public key cryptographic algorithm SM2 based on elliptic curves GB/T 37092-2018 Information security technology - Security requirements for cryptographic modules GB/T 38635 (all parts) Information security technology - Identity-based cryptographic algorithms SM9 GM/Z 4001 Cryptographic terminology IETF RFC4627 The application/json Media Type for JavaScript Object Notation (JSON)

Preview: page 2 of 5 shown, 118 in the full document. Complete English PDF, instant download:
https://chinastandards.org/standards/gm-t-0119-2022

3 Terms and Definitions for the purposes of this Document, the terms and definitions given in GM/Z 4001 and the following apply.

3.1 SM2 cryptographic algorithm an elliptic curve public key cryptographic algorithm defined by GB/T 32918 (all parts).

3.2 SM3 cryptographic algorithm A cryptographic hash algorithm defined by GB/T 32905.

3.3 SM4 cryptographic algorithm A block cipher algorithm defined by GB/T 32907.

3.4 SM9 cryptographic algorithm an identity-based asymmetric cryptographic algorithm defined by GB/T 38635 (all parts).

3.5 Industrial control system A collection of personnel, hardware and software that have an impact on the safety of industrial production processes, information security and reliable operation.

3.6 Industrial local area network the local area network that realizes the interconnection of industrial equipment has higher stability and certainty.

3.7 Programmable logic controller A digitally operated electronic system that is used in industrial environments. This system uses programmable memory as an internal register for user instructions to complete specified functions such as logic, sequence, timing, counting, calculation, etc.; and controls various types of machinery or processes through digital or analog input/output.

3.8 Programmable logic controller system A system that consists of a programmable logic controller and its related peripheral devices established by the user according to the requirements of the automation system to be completed.

3.9 Fieldbus

The digital communication technology that is applied to production sites, between field equipment and between field equipment and control devices for bidirectional, serial, multi-node.

3.10 User logic configuration Users use the tools and methods provided in the application software that supports the PLC controller to complete a collection of scripts for specific logical control tasks in the system.

3.11 User monitor configuration Users use the tools and methods provided in the application software that supports the PLC controller to complete a set of scripts for specific monitoring tasks in the system.

4 Abbreviated Terms

For the purposes of this Document, the following abbreviated terms apply.

APDU. Application Protocol Data Unit;

Preview: page 3 of 5 shown, 118 in the full document. Complete English PDF, instant download:
https://chinastandards.org/standards/gm-t-0119-2022

Chinastandards.org

PLC. Program Logic Controller

5 Overview of PLC System

5.1 Basic components the basic components of the PLC system are shown in Figure 1.See Appendix A for a detailed description of the components of the PLC control system.

e) Industrial LAN bus. Realizes LAN communication between various devices in the PLC system;

f) Fieldbus. Realizes communication between PLC controller and various field devices.

Among them, the engineer station, operator station, data service station and PLC controller are interconnected through the industrial LAN bus; the PLC controller and field devices are interconnected through the field bus.

5.2 Basic functions

The basic functions of the PLC system include.

a) Editing and developing user logic configuration;

b) Downloading user logic configuration;

c) Running user logic configuration;

d) Editing and developing user monitoring configuration;

e) Running user monitoring configuration;

f) Uploading system operation status data and events;

g) Archiving system operation status data and events;

h) Industrial LAN bus control;

i) Fieldbus control.

6 Overview of Cryptography Application in PLC System

6.1 Security lifecycle the security lifecycle of PLC system includes initialization state, programming configuration state, operation state and logout state. In different security lifecycle states, PLC system needs to use different cryptography security functions.

a) Initialization state. When the PLC system is first connected to the system network, the cryptography security initialization state is completed.

b) Programming configuration state. The PLC system is in the development state of user logic configuration and user monitoring configuration. In this state, the user can edit and test the user logic configuration and user monitoring configuration; and replace and enable the user logic configuration.

Figure 4 - Components of cryptography application system

Preview: page 4 of 5 shown, 118 in the full document. Complete English PDF, instant download:
https://chinastandards.org/standards/gm-t-0119-2022

In the PLC system, the cryptography application system mainly includes the cryptography modules and their cryptography application functions in the PLC controller, engineer station, operator station, and data service station, operator identity credentials, and security management server.

The cryptography module is embedded in each component device of the PLC system, mainly realizing the cryptographic algorithm, cryptography security function and security management function, and providing cryptography calculation service interface and security management interface to the outside world. The cryptography module can be a physical module, a software module or a hybrid module; and shall meet the security requirements specified in GB/T 37092.

The operator identity credentials are used for user login authentication on the PLC controller, engineer station, operator station and data service station.

The security management server is a background server that cooperates with the cryptography module to realize the cryptography security configuration and management of the PLC system.

In the PLC system, the cryptography module embedded in the device provides two interfaces, "cryptography security management interface" and "cryptography security service interface".

Thereof, "cryptography security management interface" exists between the device and the security management server and is used to implement cryptography security management; the "cryptography security service interface" exists inside the device and is used for business applications in the device to call cryptography security functions.

6.4 General requirements for cryptography application

6.4.1 Functional requirements the cryptography application function requirements for the PLC system are as follows.

a) The PLC system shall use the cryptographic algorithms given in Appendix C of GB/T 37092-2018, such as SM2, SM3, SM4 and SM9, etc.

b) The PLC system shall adopt a security management mechanism based on domain and state. Different application domains are isolated through cryptographic technology and configured with different keys and sensitive data. In the same application domain, different cryptography security functions are used for different security life cycle states.

c) The PLC system shall have a security management service interface to realize the registration, identity management, key configuration and cryptography security function configuration of the main equipment, applications and personnel in the system; realize the security lifecycle management of equipment and applications.

d) The key equipment such as PLC controller, operator station, engineer station in the PLC

Preview: page 5 of 5 shown, 118 in the full document. Complete English PDF, instant download:
https://chinastandards.org/standards/gm-t-0119-2022