ICS 35.030
CCS L 80

GM

# 中华人民共和国密码行业标准

GM/T 0119—2022

# PLC 控制系统及 PLC 控制器密码应用技术规范

**Cryptography applications technical specification for PLC system and PLC controller**

2022-11-20 发布　　2023-06-01 实施

国家密码管理局　　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。

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。

本文件由密码行业标准化技术委员会提出并归口。

本文件起草单位：华大半导体有限公司、中电智能科技有限公司、成都天瑞芯安科技有限公司、国家密码管理局商用密码检测中心、中国电子标准化研究院、成都密码技术研究院、北京和利时系统工程有限公司、国电南京自动化股份有限公司、广州数控设备有限公司、南方电网科学研究院有限责任公司、工业信息安全(四川)创新中心有限公司、北京华大云创科技有限公司。

本文件主要起草人：兰天、傅一帆、张兴波、尚望、张众、齐晶晶、张五一、江楠、何英武、陈剑飞、姚相振、龚洁中、杜志波、向春玲、杨祎巍、张文科、陈跃。

# PLC 控制系统及 PLC 控制器密码应用技术规范

## 1 范围

本文件描述了 PLC 控制系统和 PLC 控制器的基本组成；定义了 PLC 控制系统的密码应用功能，PLC 控制系统密码应用总体要求和密码应用基本流程；定义了 PLC 控制系统中各组成设备的密码应用功能和密码应用要求；给出了 PLC 控制系统密码应用接口参考。

本文件适用于集成密码功能的 PLC 控制系统和 PLC 控制器的设计、开发，也可用于指导相关产品的密码应用检测。

## 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。

GB/T 32905 信息安全技术 SM3 密码杂凑算法

GB/T 32907 信息安全技术 SM4 分组密码算法

GB/T 32918(所有部分) 信息安全技术 SM2 椭圆曲线公钥密码算法

GB/T 37092—2018 信息安全技术 密码模块安全要求

GB/T 38635(所有部分) 信息安全技术 SM9 标识密码算法

GM/Z 4001 密码术语

IETF RFC4627 The application/json Media Type for JavaScript Object Notation (JSON)

## 3 术语和定义

GM/Z 4001 界定的以及下列术语和定义适用于本文件。

3.1

**SM2 密码算法 SM2 cryptographic algorithm**

由 GB/T 32918(所有部分)定义的一种椭圆曲线公钥密码算法。

3.2

**SM3 密码算法 SM3 cryptographic algorithm**

由 GB/T 32905 定义的一种密码杂凑算法。

3.3

**SM4 密码算法 SM4 cryptographic algorithm**

由 GB/T 32907 定义的一种分组密码算法。

3.4

**SM9 密码算法 SM9 cryptographic algorithm**

由 GB/T 38635(所有部分)定义的一种基于身份标识的非对称密码算法。

3.5

**工业控制系统 industrial control system**

对工业生产过程安全、信息安全和可靠运行产生作用和影响的人员、硬件和软件的集合。