ICS 35.240

L 80

备案号：

T/GXIE XXXX—2025

信息系统商用密码改造技术指南

Technical guideline for the transformation of commercial

encryption in information systems

XXXX-XX-XX发布

XXXX-XX-XX实施

广西电子学会 发布

广西电子学会团体标准

目 次

[前  言 II](#_Toc14237)

[1 范围 1](#_Toc12459)

[2 规范性引用文件 1](#_Toc31683)

[3 术语和定义 1](#_Toc3298)

[4 缩略语 1](#_Toc707)

[5 通用要求 2](#_Toc25616)

[6 第二级系统密码应用指南 2](#_Toc31561)

[6.1 物理与环境改造 3](#_Toc14448)

[6.2 网络与通信改造 3](#_Toc7156)

[6.3 设备与计算改造 3](#_Toc30251)

[6.4 应用与数据改造 3](#_Toc6189)

[6.5 安全管理制度完善 4](#_Toc9058)

[7 第三级系统密码指南 4](#_Toc25731)

[7.1 物理与环境改造 4](#_Toc5523)

[7.2 网络与通信改造 4](#_Toc3838)

[7.3 设备与计算改造 5](#_Toc32540)

[7.4 应用与数据改造 5](#_Toc21266)

[7.5 安全管理制度完善 6](#_Toc32239)

[8 第四级系统密码改造指南 6](#_Toc3602)

[8.1 物理与环境改造 6](#_Toc23720)

[8.2 网络与通信改造 6](#_Toc8278)

[8.3 设备与计算改造 6](#_Toc429)

[8.4 应用与数据改造 7](#_Toc26736)

[8.5 安全管理制度完善 7](#_Toc9221)

[附 录 A 8](#_Toc12575)

[附 录 B 9](#_Toc23543)

[附 录 C 10](#_Toc28652)

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》的规则起草。

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这些专利的责任。

本文件由广西电子学会提出并归口。

本文件起草单位：。

本文件主要起草人：

信息系统商用密码改造技术指南

# 范围

本文件规定了。

本文件适用于。

# 规范性引用文件

下列文件对于本文件的应用是必不可少的。凡是注日期的引用文件，仅注日期的版本适用于本文件，凡是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 信息安全技术 SM2椭圆曲线公钥密码算法

GB/T 37092 信息安全技术 密码模块安全技术要求

GB/T 38636 信息安全技术 传输层密码协议（TLCP）

GB/T 39786 信息安全技术 信息系统密码应用基本要求

GM/T 0021 动态口令密码应用技术规范

GM/T 0022 IPSec VPN技术规范

GM/T 0024 SSL VPN技术规范

GM/T 0027 智能密码钥匙技术规范

GM/T 0028 密码模块安全技术要求

GM/T 0036 采用非接触卡的门禁系统密码应用技术指南

GM/Z 4001 密码术语

# 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。

# 缩略语

下列缩略语适用于本文件。

# 通用要求

# 第二级系统密码应用指南

## 物理与环境改造

### 身份鉴别

### 电子门禁记录数据存储完整性

### 视频监控记录数据存储完整性

## 网络与通信改造

### 身份鉴别

### 通信数据完整性

### 通信过程中重要数据的机密性

### 网络边界访问控制信息的完整性

### 安全接入认证

## 设备与计算改造

### 身份鉴别

### 远程管理通道安全

### 系统资源访问控制信息完整性

### 日志记录完整性

### 重要可执行程序完整性、重要可执行程序完整性

## 应用与数据改造

### 身份鉴别

### 访问控制信息完整性

### 重要信息资源安全标记完整性

### 重要数据传输机密性

### 重要数据存储机密性

### 重要数据传输完整性

### 重要数据传输完整性

### 不可否认性

## 安全管理制度完善

### 管理制度

### 人员管理

### 建设运行

### 应急处置

# 第三级系统密码指南

## 物理与环境改造

### 身份鉴别

### 电子门禁记录数据存储完整性

### 视频监控记录数据存储完整性

## 网络与通信改造

### 身份鉴别

### 通信数据完整性

### 通信过程中重要数据的机密性

### 网络边界访问控制信息的完整性

### 安全接入认证

## 设备与计算改造

### 身份鉴别

### 远程管理通道安全

### 系统资源访问控制信息完整性

### 日志记录完整性

### 重要可执行程序完整性、重要可执行程序完整性

## 应用与数据改造

### 身份鉴别

### 访问控制信息完整性

### 重要信息资源安全标记完整性

### 重要数据传输机密性

### 重要数据存储机密性

### 重要数据传输完整性

### 重要数据传输完整性

### 不可否认性

## 安全管理制度完善

### 管理制度

### 人员管理

### 建设运行

### 应急处置

# 第四级系统密码改造指南

## 物理与环境改造

### 身份鉴别

### 电子门禁记录数据存储完整性

### 视频监控记录数据存储完整性

## 网络与通信改造

### 身份鉴别

### 通信数据完整性

### 通信过程中重要数据的机密性

### 网络边界访问控制信息的完整性

### 安全接入认证

## 设备与计算改造

### 身份鉴别

### 远程管理通道安全

### 系统资源访问控制信息完整性

### 日志记录完整性

### 重要可执行程序完整性、重要可执行程序完整性

## 应用与数据改造

### 身份鉴别

### 访问控制信息完整性

### 重要信息资源安全标记完整性

### 重要数据传输机密性

### 重要数据存储机密性

### 重要数据传输完整性

### 重要数据传输完整性

### 不可否认性

## 安全管理制度完善

### 管理制度

### 人员管理

### 建设运行

### 应急处置

# 附 录 A

（资料性附录）

第二、三、四级别系统密码改造差异对照表

# 附 录 B

（资料性附录）

政务云上应用系统改造说明

# 附 录 C

（资料性附录）

重要数据分类参考表