ICS 35.030
CCS L 80

中华人民共和国密码行业标准

GM/T 0133—2024

关键信息基础设施密码应用要求

Requirements for critical information infrastructure cryptography application

2024-12-27 发布　　2025-07-01 实施

国家密码管理局　　发布

目　　次

前言 …… Ⅲ
引言 …… Ⅳ
1　范围 …… 1
2　规范性引用文件 …… 1
3　术语和定义 …… 1
4　缩略语 …… 2
5　总体原则 …… 2
6　密码应用实施要求 …… 2
6.1　密码应用规划 …… 2
6.2　密码应用建设 …… 3
6.3　密码应用运行 …… 3
6.4　密码应用安全性评估 …… 3
7　密码应用技术和管理要求 …… 4
7.1　基本要求 …… 4
7.2　增强技术要求 …… 4
7.2.1　网络和通信安全 …… 4
7.2.2　设备和计算安全 …… 4
7.2.3　应用和数据安全 …… 5
7.3　增强管理要求 …… 5
7.3.1　人员管理 …… 5
7.3.2　建设运行 …… 5
7.3.3　密码产品和服务 …… 6
7.3.4　密钥管理 …… 6
8　密码运行安全保障要求 …… 6
8.1　密码资源弹性供给 …… 6
8.2　密码运行状态监测预警 …… 6
8.3　密码运行安全事件应急处置 …… 6
附录 A（资料性）　关键信息基础设施密码应用要求汇总列表 …… 8
参考文献 …… 11

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：北京数字认证股份有限公司、公安部第三研究所、中国科学院信息工程研究所、北京市经济和信息化局网络安全管理中心、中国科学院大学、兴唐通信科技有限公司、华为技术有限公司、中电科网络安全科技股份有限公司、商用密码检测认证中心、中国移动通信集团有限公司、国家计算机网络应急技术处理协调中心、昆仑数智科技有限责任公司、中国电子科技集团公司第十五研究所、中国石油化工集团有限公司、上海证券交易所、上交所技术有限责任公司、中互金认证有限公司、公安部第一研究所、中科信息安全共性技术国家工程研究中心有限公司、中国电力科学研究院有限公司、上海交通大学、鼎铉商用密码测评技术（深圳）有限公司、教育部教育管理信息中心、中国电子技术标准化研究院、中国信息通信研究院、国家信息中心、中国工业互联网研究院、中国金融电子化集团有限公司、中国工商银行股份有限公司、中国国家铁路集团有限公司科技和信息化部、中电信数智科技有限公司、天翼云科技有限公司、联通智慧安全科技有限公司、深圳市网安计算机安全检测技术有限公司、长春吉大正元信息技术股份有限公司、三未信安科技股份有限公司。

本文件主要起草人：夏冰冰、詹榜华、林雪焰、陈海虹、李佳曦、王晗、王佳欢、夏鲁宁、杜皎、张永强、黎水林、王勇、贾世杰、马原、陈天宇、赵阳、郑昉昱、刘尚焱、邵萌、彭红、张立廷、罗鹏、张立花、张艳、张晓娜、张嵩、刘健、杨龙、黄喆磊、朱立、房慧丽、李增局、李秋香、刘志宇、周世杰、胡建勋、高振鹏、李智虎、银鹰、陈磊、肖飞、张鹏、黄晶晶、徐秀、罗海宁、查奇文、李振、李萌、张文塔、王建峰、刘乐、南杰慧、邓诗智、赵丽丽、高志权。

引　言

为落实《中华人民共和国网络安全法》《中华人民共和国密码法》《商用密码管理条例》《关键信息基础设施安全保护条例》中的相关要求，保障关键信息基础设施的安全稳定运行，关键信息基础设施的安全保护建设在遵循 GB/T 39204—2022《信息安全技术　关键信息基础设施安全保护要求》的前提下，采用密码技术对关键信息基础设施实施合规、正确、有效的保护，实现体系化密码应用。

总体而言，关键信息基础设施运营者开展密码应用工作时，在遵循 GB/T 39786—2021《信息安全技术　信息系统密码应用基本要求》的基础上，重点考虑关键业务在稳定性、业务持续性方面的保障要求，从整体视角出发分析识别关键业务所面临的安全风险，落实本文件中提出的对关键信息基础设施实施重点保护所需的密码应用实施要求、密码应用技术和管理要求以及密码运行安全保障要求，切实保障关键信息基础设施安全稳定运行。

关键信息基础设施密码应用要求

1 范围

本文件规定了关键信息基础设施的密码应用实施要求、密码应用技术和管理要求、密码运行安全保障要求。

本文件适用于指导和规范关键信息基础设施运营者对关键信息基础设施密码应用的规划、建设、运行及安全性评估，也可供关键信息基础设施安全保护的其他相关方参考使用。

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 22239—2019 信息安全技术 网络安全等级保护基本要求

GB/T 25069—2022 信息安全技术 术语

GB/T 39204—2022 信息安全技术 关键信息基础设施安全保护要求

GB/T 39786—2021 信息安全技术 信息系统密码应用基本要求

3 术语和定义

GB/T 22239—2019、GB/T 25069—2022、GB/T 39204—2022、GB/T 39786—2021 界定的以及下列术语和定义适用于本文件。

3.1

关键信息基础设施 critical information infrastructure

公共通信和信息服务、能源、交通、水利、金融、公共服务、电子政务、国防科技工业等重要行业和领域，以及其他一旦遭到破坏、丧失功能或者数据泄露，可能严重危害国家安全、国计民生、公共利益的重要网络设施、信息系统等。

[来源：GB/T 39204—2022，3.1]

3.2

关键信息基础设施边界 critical information infrastructure boundary

所有关键信息基础设施要素的集合。

3.3

商用密码保障系统 cryptographic security system

通过商用密码算法、密码协议、密钥管理机制等密码技术实现，能够提供一种或多种密码功能，用于保障网络和信息系统安全稳定运行并维护身份真实性、数据的完整性和机密性、行为不可否认性的系统。

注：密码功能包括但不限于加密传输、加密存储、数字签名、密钥管理等。

3.4

重要数据 key data

特定领域、特定群体、特定区域或达到一定精度和规模的，一旦被泄露或篡改、损毁，可能直接危害

国家安全、经济运行、社会稳定、公共健康和安全的数据。

注：仅影响组织自身或公民个体的数据一般不作为重要数据。

[来源：GB/T 43697—2024，3.2]

3.5

核心数据　core data

对领域、群体、区域具有较高覆盖度或达到较高精度、较大规模、一定深度的，一旦被非法使用或共享，可能直接影响政治安全的重要数据。

注：核心数据主要包括关系国家安全重点领域的数据，关系国民经济命脉、重要民生、重大公共利益的数据，国家有关部门评估确定的其他数据。

[来源：GB/T 43697—2024，3.3]

3.6

敏感个人信息　sensitive personal information

一旦泄露或者非法使用，容易导致自然人的人格尊严受到侵害或者人身、财产安全受到危害的个人信息。

[来源：GB/T 43697—2024，3.6]

3.7

网络隔离产品　network separation products

位于两个不同安全域之间，采用协议隔离技术在网络上实现安全域安全隔离与信息交换的产品。

[来源：GB/T 20279—2015，3.8]

4　缩略语

下列缩略语适用于本文件。

SLA：服务等级协议（Service Level Agreement）

5　总体原则

关键信息基础设施密码应用在边界内各等级保护对象符合 GB/T 39786—2021 密码应用基本要求的基础上，依据以下原则开展整体密码应用工作。

——规范性：关键信息基础设施密码应用实施各环节的关键活动符合密码相关法律法规，实现密码应用规划、建设、运行及安全性评估的闭环过程。

——系统性：立足关键信息基础设施整体视角，以风险管理为导向，识别密码应用需求，构建体系化的密码保障能力。

——健壮性：建设密码运行安全保障能力，确保商用密码保障系统满足关键业务的可靠性和可用性要求，保障关键信息基础设施安全稳定运行。

本文件的主要内容包括：

——密码应用实施要求，

——密码应用技术和管理要求，

——密码运行安全保障要求。

本文件与 GB/T 39786—2021 的对照关系见附录 A。

6　密码应用实施要求

6.1　密码应用规划

本项要求包括以下内容。

a) 应形成关键信息基础设施资产清单，分析关键业务运行过程中面临的安全风险，综合已具备的安全控制措施（例如访问控制、审计等）和管理制度、关键信息基础设施的网络/计算/存储能力、关键业务连续运行时间和业务峰值要求等因素，统筹确定体系化的密码应用需求。

注 1：关键信息基础设施资产清单包括但不限于物理/网络/设备/应用/数据和其他类资产的名称、类别、资产重要性、支撑业务的重要性、资产防护的优先级等。

b) 应对关键信息基础设施的密码应用进行统筹规划和顶层设计，制定关键信息基础设施商用密码应用方案，方案内容包括但不限于：

1) 关键信息基础设施密码应用需求；

2) 关键信息基础设施密码应用设计，包括但不限于密码应用总体架构，密码应用技术和管理措施，商用密码保障系统的资源供给模式，密钥管理职责划分和密钥全生命周期管理，密码运行状态监测预警策略，密码运行安全事件应急处置策略等；

注 2：资源供给模式包括但不限于资源共享/独享策略、资源调配策略、冗余备份策略等。

注 3：密钥全生命周期管理包括但不限于密钥使用用途、密钥更新周期、密钥备份原则、管理密钥人员要求等。

3) 关键信息基础设施商用密码保障系统的设计建设模式、建设周期、阶段划分、各阶段建设目标；

注 4：设计建设模式包括但不限于整体统一设计建设、各等级保护对象分别设计建设等。

4) 关键信息基础设施商用密码应用方案的使用、流转范围。

c) 在关键信息基础设施发生改建、扩建、所有人变更等较大变化时，应重新开展密码应用需求分析、方案设计等工作。

6.2 密码应用建设

本项要求包括以下内容。

a) 应明确密码应用建设实施范围。

b) 应根据关键信息基础设施商用密码应用方案开展密码应用建设活动。

c) 密码应用建设活动应包括但不限于：

1) 明确密码产品与服务采购清单，根据采购清单对密码产品和服务进行采购；

2) 密码产品和服务与各种应用系统的正确、合规、有效集成；

3) 落实密码应用管理措施；

4) 对密码应用建设活动的质量、进度、文档和变更工作进行监督控制和科学管理等。

6.3 密码应用运行

本项要求包括：

a) 应根据关键信息基础设施商用密码应用方案执行关键信息基础设施密码应用运行的技术措施和管理措施等；

b) 当密码应用被转移、终止或废弃时，应采取安全可靠的方法进行密钥等数据转移、暂存和清除，密码产品迁移或废弃，相关存储介质的清除或销毁等。

6.4 密码应用安全性评估

本项要求包括以下内容。

a) 关键信息基础设施商用密码应用方案的商用密码应用安全性评估应遵循以下要求：

1) 对关键信息基础设施商用密码应用方案进行商用密码应用安全性评估，未通过评估的不得作为密码应用建设的依据；

2) 建设过程中需要调整商用密码应用方案的，重新组织评估，通过后方可根据调整后的方案

继续建设。

b） 关键信息基础设施的商用密码应用安全性评估应遵循以下要求：

1） 新建关键信息基础设施投入运行前，进行商用密码应用安全性评估，评估通过后方可投入运行；

2） 已投入运行的关键信息基础设施，在运行期间每年至少开展一次商用密码应用安全性评估；

3） 对未通过评估的关键信息基础设施，运营者进行整改；确因客观原因短期内无法完成整改的，采取必要措施保障关键信息基础设施运行安全。

c） 应根据密码相关法律、行政法规和国家有关规定要求汇总留存和管理评估情况。

7 密码应用技术和管理要求

7.1 基本要求

关键信息基础设施边界内各等级保护对象，应按照自身的安全保护等级符合 GB/T 39786—2021 的要求：

——通用要求，

——物理和环境安全，

——网络和通信安全，

——设备和计算安全，

——应用和数据安全，

——管理制度，

——人员管理，

——建设运行，

——应急处置。

关键信息基础设施边界内各等级保护对象应符合相应行业标准的要求。

7.2 增强技术要求

7.2.1 网络和通信安全

本项要求包括：

a） 关键信息基础设施边界内各等级保护对象之间进行网络通信时，应采用密码技术对通信双方实体进行身份鉴别、并保护通信过程中数据的机密性和完整性；

b） 关键信息基础设施边界内等级保护对象与边界外等级保护对象之间进行网络通信时，应采用密码技术对通信双方实体进行身份鉴别、对数据交换和信息流向进行控制、并保护通信过程中数据的机密性和完整性。

注 1：等级保护对象包括单个完整的等级保护对象，以及单个等级保护对象中被划定在关键信息基础设施边界内的部分组成要素。

注 2：通信双方实体可能涉及设备、应用系统等。

7.2.2 设备和计算安全

本项要求包括：

a） 对使用的密码产品和服务进行运维管理时，应形成针对重要运维操作的日志，采用密码技术保护日志记录的完整性；

b） 应采用密码技术保护重要可执行程序内容和版本信息的完整性，并验证其来源真实性。

注：重要可执行程序包括但不限于可执行程序、执行依赖程序、涉及软件或固件远程更新的程序等。

7.2.3 应用和数据安全

7.2.3.1 应用安全

本项要求包括：

a） 应采用密码技术保护重要操作行为的访问控制信息和操作行为记录的完整性；

b） 在可能涉及法律责任认定的应用中，应采用密码技术实现重要操作行为的不可否认性。

注：重要操作行为包括但不限于重要业务操作、重要用户操作或异常用户操作等。

7.2.3.2 数据安全

本项要求包括：

a） 应采用密码技术验证收集的核心数据、重要数据和敏感个人信息的来源真实性；

b） 应采用密码技术保护核心数据、重要数据和敏感个人信息在存储过程中的机密性和完整性；对于核心数据，严格管理密码产品和服务提供的数据解密功能的操作权限，将数据解密相关操作纳入重要业务操作范围进行审计；

c） 核心数据、重要数据和敏感个人信息在关键信息基础设施边界内各等级保护对象之间直接流动或通过网络隔离产品流动时，以及跨边界直接流动或通过网络隔离产品流动时，应采用密码技术保护数据的机密性和完整性。

7.3 增强管理要求

7.3.1 人员管理

本项要求包括：

a） 密码应用岗位人员应根据密码相关法律、行政法规和国家有关规定要求，具备相应的专业学历或职业技能；

b） 应在密码应用岗位人员任前进行背景审查，并留存审查结果记录；

c） 在密码应用岗位人员发生岗位调动时，应重新评估和修改其访问权限和职责；

d） 在密码应用岗位人员离职时，应及时终止其所有密码应用相关的访问权限、操作权限，收回相应的密码产品，并根据密钥管理策略处理相关密钥数据。

7.3.2 建设运行

本项要求包括以下内容。

a） 应按照 6.2 和 6.3 中的内容开展密码应用建设运行。

b） 攻防对抗演习应遵循以下要求：

1） 根据保护工作部门的要求明确攻防对抗演习组织形式、进度安排、资源保障等；

2） 明确攻防对抗演习具体内容，包括但不限于分析识别密码应用脆弱性，开展验证或模拟攻击和防御；

注：密码应用脆弱性包括但不限于密码功能被旁路、密码产品和服务错误配置、用户非法操作导致的问题等。

3） 定期开展攻防对抗演习，针对密码应用攻防对抗演习中发现的问题及时进行整改。

c） 供应链安全建设应遵循以下要求：

1） 采购密码产品和服务时，符合 GB/T 39204—2022 中 7.9 a）、c）、d）、g）、k）的相关要求；

2） 与密码服务的供应方签订服务等级协议（SLA），明确职责划分和对密码服务供应方的要

求，包括但不限于密码服务的连续性、安全性、合规性等方面的要求；

3） 梳理底层基础软硬件产品代码签名机制的潜在安全风险，将风险及缓解措施纳入应急预案，当发生异常情况时，会同密码产品和服务供应方及时采取风险缓解措施。

d） 安全运维管理应遵循以下要求：

1） 对密码产品和服务进行运维时，符合 GB/T 39204—2022 中 7.8 的相关要求；

2） 根据关键信息基础设施商用密码保障系统的设计建设模式、资源供给模式对密码产品和服务的策略配置、补丁升级等相关事项进行集中管理。

e） 应根据密码相关法律、行政法规和国家有关规定要求报告关键信息基础设施商用密码使用情况。

7.3.3 密码产品和服务

法律、行政法规和国家有关规定要求使用商用密码进行保护的关键信息基础设施，使用的商用密码产品、服务应经检测认证合格，使用的密码算法、密码协议、密钥管理机制等商用密码技术应通过国家密码管理部门审查鉴定。

7.3.4 密钥管理

本项要求包括：

a） 应保证密钥数据生命周期的安全性，确保公钥不被非授权修改和替换，除公钥外的其他密钥不被非授权访问、使用、泄露、修改和替换；

b） 应根据密钥管理策略进行密钥使用，保证不同业务应用、不同类型和级别的数据使用不同的密钥；

c） 应根据密钥管理策略执行密钥更新；

d） 应根据密钥管理策略执行密钥备份，保证密钥的可用性。

8 密码运行安全保障要求

8.1 密码资源弹性供给

本项要求包括：

a） 应根据 6.1 b)中的资源调配策略，对关键信息基础设施使用的密码资源进行调配；

b） 应根据 6.1 b)中的冗余备份策略，支持在必要时(例如密码产品功能中断等)切换到冗余备份产品。

8.2 密码运行状态监测预警

本项要求包括：

a） 应根据 6.1 b)中的监测预警策略对密码运行状态进行监测，基于监测数据进行分析研判和预警；

b） 应采用密码技术保护监测数据和预警信息的完整性，验证其来源真实性；

c） 对于监测数据和预警信息中涉及的核心数据、重要数据和敏感个人信息，应符合 7.2.3.2 的相关要求。

8.3 密码运行安全事件应急处置

本项要求包括：

a） 应根据 6.1 b)中的应急处置策略制定针对密码运行安全事件的应急预案，内容包括但不限于

事件分类分级、预案启动条件、应急组织构成、事件报告流程、信息共享机制、处置恢复流程、应急资源保障、演练和培训等；

b） 应根据应急预案定期开展应急演练活动；

c） 应根据应急预案对已发生的密码运行安全事件实施分类分级处置，并形成事件处置记录；

d） 应根据法律、行政法规和国家有关规定要求，参与和配合保护工作部门开展的应急处置工作；

e） 应根据应急预案将事件通知到可能受影响的内部部门和人员，以及供应链涉及的、与事件相关的其他外部组织；

f） 应根据密码相关法律、行政法规和国家有关规定要求，开展密码运行安全事件及其处置情况报告工作；

g） 应建立和完善密码运行安全事件应对知识库，包括但不限于历史安全事件经验、事件应对措施等；

h） 应将应急预案纳入密码应用岗位人员的培训和考核内容。

附 录 A
（资料性）
关键信息基础设施密码应用要求汇总列表

关键信息基础设施密码应用要求汇总列表见表 A.1。

表 A.1 关键信息基础设施密码应用要求汇总列表

指标维度		关键信息基础设施边界内各等级保护对象符合 GB/T 39786—2021 的对应级别要求	关键信息基础设施整体应遵循的补充和增强要求
密码应用实施要求	密码应用规划	见 GB/T 39786—2021 中的“建设运行”	明确密码应用需求分析
			明确关键信息基础设施商用密码应用方案内容
			重大变化重新开展需求分析、方案设计
	密码应用建设		根据商用密码应用方案进行建设
			明确建设范围
			明确实施内容
	密码应用运行		明确运行环节要求
			明确终止环节要求
	密码应用安全性评估		关键信息基础设施商用密码应用方案评估
			关键信息基础设施的运行前评估、定期评估、评估后整改
			评估情况汇总
密码应用技术和管理要求	基本要求	—	关键信息基础设施边界内各等级保护对象符合 GB/T 39786—2021 和其他相应行业标准要求
	物理和环境安全	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	
	网络和通信安全	身份鉴别	细化保护对象
		通信数据完整性	细化保护对象并补充数据交换和信息流向控制要求
		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	

表 A.1　关键信息基础设施密码应用要求汇总列表（续）

指标维度		关键信息基础设施边界内各等级保护对象符合 GB/T 39786—2021 的对应级别要求	关键信息基础设施整体应遵循的补充和增强要求
密码应用技术和管理要求	设备和计算安全	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	
		重要信息资源安全标记完整性	
		日志记录完整性	细化保护对象并增强完整性要求
		重要可执行程序完整性和来源真实性	细化保护对象并增强完整性要求
	应用和数据安全	身份鉴别	—
		访问控制信息完整性	细化保护对象并增强完整性要求
		重要信息资源安全标记完整性	—
		重要数据传输机密性	细化保护对象
		重要数据传输完整性	
		重要数据存储机密性	细化保护对象
		重要数据存储完整性	
		不可否认性	增强不可否认性要求
		—	补充来源真实性要求
	人员管理	了解并遵守密码相关法律法规和密码管理制度	—
		建立密码应用岗位责任制度	补充专职人员配置要求
		建立上岗人员培训制度	—
		定期进行安全岗位人员考核	
		建立关键岗位人员保密制度和调离制度	增强背景审查要求
			补充岗位调整管理要求
			补充离职管理要求
	建设运行	制定商用密码应用方案	补充攻防对抗演习要求 补充供应链安全建设要求 补充安全运维管理要求
		制定密钥安全管理策略	
		制定实施方案	
		投入运行前进行商用密码应用安全性评估	
		定期开展商用密码应用安全性评估及攻防对抗演习	
	密码产品和服务	见 GB/T 39786—2021 中的“通用要求”	密码产品、服务的检测认证和密码技术经审查鉴定

表 A.1　关键信息基础设施密码应用要求汇总列表（续）

指标维度		关键信息基础设施边界内各等级保护对象符合 GB/T 39786—2021 的对应级别要求	关键信息基础设施整体应遵循的补充和增强要求
密码应用技术和管理要求	密钥管理	见 GB/T 39786—2021 中的“建设运行”“管理制度”及“附录 B”	补充保证全生命周期安全要求
			补充密钥专用要求
			补充密钥更新要求
			补充密钥备份要求
	管理制度	具备密码应用安全管理制度	—
		密钥管理规则	见本文件中的“密钥管理”
		建立操作规范	—
		定期修订安全管理制度	
		明确管理制度发布流程	
		制度执行过程记录留存	
	应急处置	应急策略	见本文件中的“密码运行安全事件应急处置”
		事件处置	
		向有关主管部门上报处置情况	
密码运行安全保障要求	密码资源弹性供给	—	补充密码资源调配要求
			补充密码资源冗余备份要求
	密码运行状态监测预警		补充监测预警要求
			补充监测预警信息完整性、来源真实性要求
			补充监测预警信息中的数据安全要求
	密码运行安全事件应急处置	见 GB/T 39786—2021 中的“应急处置”	补充应急预案编制要求
			补充定期开展应急演练活动要求
			补充事件分类分级并记录要求
			补充应急处置要求
			补充事件通知要求
			补充处置情况报告要求
			补充完善知识库要求
			补充纳入考核和培训要求

参 考 文 献

[1] GB/T 20279—2015 信息安全技术 网络和终端隔离产品安全技术要求

[2] GB/T 43269—2023 信息安全技术 网络安全应急能力评估准则

[3] GB/T 43697—2024 数据安全技术 数据分类分级规则

[4] GM/T 0132—2023 信息系统密码应用实施指南

[5] 中华人民共和国网络安全法(2016 年 11 月 7 日第十二届全国人民代表大会常务委员会第二十四次会议通过)

[6] 中华人民共和国密码法(2019 年 10 月 26 日第十三届全国人民代表大会常务委员会第十四次会议通过)

[7] 中华人民共和国数据安全法(2021 年 6 月 10 日第十三届全国人民代表大会常务委员会第二十九次会议通过)

[8] 中华人民共和国个人信息保护法(2021 年 8 月 20 日第十三届全国人民代表大会常务委员会第三十次会议通过)

[9] 关键信息基础设施安全保护条例(2021 年 4 月 27 日国务院第 133 次常务会议通过,中华人民共和国国务院令第 745 号)

[10] 商用密码管理条例(2023 年 4 月 14 日国务院第 4 次常务会议修订通过,中华人民共和国国务院令第 760 号)

[11] 商用密码应用安全性评估管理办法(2023 年 9 月 11 日国家密码管理局局务会议审议通过,国家密码管理局令第 3 号)

[12] 贯彻落实网络安全等级保护制度和关键信息基础设施安全保护制度的指导意见(2020 年 7 月 22 日公安部公网安〔2020〕1960 号)

中华人民共和国密码
行业标准
关键信息基础设施密码应用要求
GM/T 0133—2024
*
中国标准出版社出版发行
北京市朝阳区和平里西街甲2号(100029)
网址 www.spc.net.cn
总编室:(010)68533533　发行中心:(010)51780238
读者服务部:(010)68523946
中国标准出版社秦皇岛印刷厂印刷
各地新华书店经销
*
开本 880×1230　1/16　印张 1.25　字数 25 千字
2025年6月第1版　2025年6月第1次印刷
*
书号:155066·2-39069　定价 38.00 元

GM/T 0133-2024