民航行业标准
《民用航空重要网络和信息系统商用密码应用要求》
（征求意见稿）

编制说明

《民用航空重要网络和信息系统商用密码应用要求》

编制组

2026 年 7 月

一、工作简况

（一）任务来源

《民用航空重要信息系统商用密码应用要求》为2025年计划内标准项目，标准编制周期为12个月。该标准由中国民用航空局综合司提出，牵头起草单位为中国航空油料集团有限公司。

（二）主要起草单位和工作组成员

主要起草单位：中国航空油料集团有限公司、中国民航信息网络股份有限公司、河南省机场集团有限公司、中国民用航空西南地区空中交通管理局、中国民用航空总局第二研究所、中国国际航空股份有限公司、北京海泰方圆科技股份有限公司、中电科网络安全科技股份有限公司、中国电子技术标准化研究院、国家计算机网络应急技术处理协调中心、国家商用密码应用技术研究工程中心等。

编制组成员：夏伟、李绪国、周子站、李辛阳、苏力行、项熙艳、王欣、张韶华、宁文冠、龚丽、郭睿、翟冬梅、罗影、焦亨炼、黄晶晶、张晓娜、王亮、张东海、陈彦平等。

（三）标准制定的背景、目的和意义

当前复杂多变的国际形势下，我国网络和数据安全问题凸显，民用航空作为国民经济的重要领域，拥有数量众多的网络安全等级保护三级及以上信息系统和关键信息基础设施，承担着航班飞行管控、机场安检、旅客管理、航油加注、航司值机等重要业务，系统间数据交互频繁，安

全责任链条复杂。商用密码技术作为保障网络和数据安全的核心技术，是民用航空业安全保护和信任体系建设的基础。民用航空业在商用密码应用方面仍面临诸多挑战，主要表现为：一是多数关键业务数据未进行加密存储防护，航班调度、离港控制等核心业务系统对密码技术的融合仍停留在局部加密层面，尚未形成覆盖数据全生命周期的防护体系，网络传输也未完全采用专用加密措施；二是系统低延迟、高吞吐的特性对密码产品性能要求严格，现有密码产品未经充分验证，存在与老旧系统和云环境等重要系统的适配风险；三是商密应用改造责任难以界定，不同单位协同运行的行业模式难以落实商用密码应用安全主体责任。

当前，民航业正加快数字化转型，广泛应用物联网、大数据、人工智能等新技术，借助本标准，制定覆盖全业务环节的商密应用适用性标准体系，推动密码技术规范化、系统化应用，全面落实《中华人民共和国网络安全法》《中华人民共和国数据安全法》《中华人民共和国密码法》《商用密码应用安全性评估管理办法》等法规、规章要求，以商用密码为重要技术防线，构建统一的安全标准体系，可有效提升行业安全治理能力，支撑“十四五”战略目标落实，保障民航数字化转型安全可靠。

（四）主要工作过程

1. 组建编制组

2024 年 3 月，成立标准编制组，搜集相关材料，开展标准立项前期研究工作。

2. 前期调研

（1）2024 年 4 月，中国航空油料集团有限公司（以下简称“中国航油”）、中国民用航空总局第二研究所、中国民航信息网络股份有限公司、中国民航大学等行业内单位在成都召开标准立项研讨会，中国民航科学技术研究院（以下简称“航科院”）参加研讨，对项目立项的必要性和需求进行深入研讨和论证，初步明确了标准编制思路;

（2）2024 年 5 月，中国航油组织标准编制组研究编制并提交了立项申报建议书和标准草案。

3. 开题评审

2025 年 5 月 16 日，航科院在北京组织召开标准开题评审会，评审组听取了项目承担单位中国航油的项目汇报，对项目的必要性、可行性、主要内容、工作计划、项目预期成果以及承担单位的能力等方面进行评审，一致认为该项目目标明确、内容全面、技术方案可行、实施计划合理，同意该项目开题。

4. 标准起草

（1）2025 年 6 月 11 日，编制组召开了标准制定启动会，通报了项目立项批复情况，中国航空油料集团有限公司代表项目组介绍了标准编制思路、任务分工和时间计划安排，并与各参编单位充分讨论。

（2）2025 年 6～7 月，编制组赴四川天府机场集团、广州白云机场集团和南方航空集团现场调研商用密码应用现状与需求，组织召开由行业用户和网络安全服务机构参加的研讨会议，探讨标准编制技术路线和指标体系；

（3）2025 年 7 月，编制组赴民航局综合司，就标准研制工作思路听取综合司意见和要求，开始编制《民用航空重要信息系统密码应用现状与需求分析报告》。

（4）2025 年 8 月 13 日，中国航油组织标准编制工作研讨会，各参编单位现场参加，重点就前期调研情况进行研讨，进一步明确了标准（初稿）编制思路。

（5）2025 年 8 月～2025 年 12 月，编制组集中编制，并形成标准（初稿）。期间，编制组还赴拉萨机场调研，进一步了解商密应用过程中存在的突出问题和解决建议。

（6）2026 年 1 月 27 日，中国航油组织召开专家研讨会，邀请行业内外专家、民航局综合司和国家密码管理局有关处室领导现场参会，充分听取专家意见。

（7）2026 年 2 月～3 月，编制组针对 1 月 27 日专家意见深入研讨，进一步修改完善标准（初稿）内容，并形成标准（征求意见稿）初稿。

（8）2026 年 5 月 15 日，航科院组织召开标准技术（中期）评审会。评审组听取标准起草单位汇报并逐条评审，一致同意通过评审，建议标准起草单位尽快根据专家意见进行修改完善，形成标准征求意见稿，广泛征求意见。

（9）2026 年 5 月 16 日～6 月 15 日，标准编写组按照专家评审意见集中逐条核对标准条款内容，确保在与《信息系统密码应用基本要求》（GB/T 39786—2021）内容要求保持一致基础上提出行业针对性要求，简化基本要求、增强要求内容并提高适用性，增设关键信息基础设施扩展要求章节，将标准名称修改为《民用航空重要网络和信息系统商用密码应用要求》，完善附录 A“商用密码应用保护对象和应用场景”内容，形成标准征求意见稿。

二、编写原则和主要内容（如技术指标、参数、公式、性能要求、试验方法、试验规则等）的编写论据（包括计算、测试、统计等数据），修订标准时应说明主要技术内容的修改情况

（一）标准编写原则

本标准在编制过程中遵循了针对性和前瞻性原则。

1. 针对性原则

体现在与实际情况相结合。编制组在充分调研相关国内标准内容基础上，结合民航业重要信息系统商密应用现状和存在问题，统筹平衡各方要求，考虑标准要求的普适性和合理性，针对民航空管、客票、行李、加油等民用航空重要信息系统的高安全需求特性，在密码系统建设、使用和运维等方面研究提出针对性的技术要求，确保所选技术和产品符合系统运行特点，解决密码应用领域硬件设备依赖程度高、维护成本高等突出问题，有效提升数据的安全性，避免发生数据泄露和被窃取现象。

2. 前瞻性原则

体现在与密码应用相结合。标准编制过程中，工作组充分考虑国家密码法等法律法规以及公安部、民航局等相关要求落地实施，充分考虑密码在系统和数据保护等方面的突出优势，标准中所要求的SM2数字签名算法、SM3密码杂凑算法、祖冲之（ZUC）序列密码算法、SM4分组密码算法、SM9标识密码算法均已正式发布为ISO/IEC国际标准，强调密码防护技术的高可靠性、安全性，使用系统可靠性、低延时等要求，充分体现民航特点。标准落地实施后，商用密码技术在民用航空信息系统中的应用将会带来创新性的安全措施和解决方案，将密码技术融入系统设计、研发和运行维护的全过程，也将衍生出新安全防护策略，体现密码应用技术标准的创新性。

（二）标准主要内容

本文件共包括10章正文。

第1、2、3和4章为标准的常规性描述，包括范围、规范性引用文件、术语和定义、缩略语。

第5章提出商用密码应用保护对象和应用强度。同时在附录A中给出了空中交通管理类系统等不同类型的业务系统有关保障数据的机密性、完整性保护对象，信息系统有关实体身份的真实性应用场景，以及操作行为数据不可否认性保护对象。

第6章提出商用密码应用基本要求，具体包括物理环境安全、网络与通信安全、设备与计算安全、应用和数据

安全、管理制度、人员管理、建设运行、应急处置、密钥管理以及安全审计等方面内容，适用于网络安全保护第三级及以上的网络和信息系统、相应保护等级的关键信息基础设施。

第7章提出商用密码应用增强要求，与第6章内容相比，未涉及密钥管理有关内容，适用于网络安全保护第四级及以上的网络和信息系统、相应保护等级的关键信息基础设施。

第8章针对关键信息基础设施，结合《关键信息基础设施密码应用要求》（GM/T 0133—2024）等有关标准，提出针对性扩展要求。

第9章针对商用密码产品自身的合规性、可靠性、安全性、稳定性、实时性等方面提出要求，同时，在附录B中列出了密码机、密钥管理类产品、身份认证类产品、综合网关类产品以及工业控制专用密码产品等典型密码产品的核心性能指标，并作为资料性附录，以供有关单位更好地理解和选择密码产品。

第10章从行业监管角度对商用密码应用安全性评估和整改等提出管理要求。

（三）修订标准新、旧版本主要技术内容改变的说明

无。

三、是否涉及专利，涉及专利的，说明专利名称、编号及相关信息

本标准不涉及专利。

四、主要试验或验证的分析、综述报告、技术论证、预期的经济效益和社会效益

（一）主要试验或验证的分析、综述报告、技术论证

本标准在充分调研论证行业现状、存在问题和需求的基础上，总结凝练而成，未开展试验或验证工作。

（二）预期的经济效益

从产业规模来看，我国商用密码产业近年来显著增长。根据相关数据，2021 年商用密码产业规模达到 585 亿元人民币，预计在 2026 年将增至 1300 亿元，反映出商用密码产业的强劲发展势头和广阔的市场前景。本标准总结民航领域管理和业务应用的特殊需求，并进行专门设计，填补了民航领域信息系统体系化密码应用标准的空白，可以更好地适配民航相关业务场景，并全面支持目前云、大、物、移、智、链等新技术体系下的密码应用，促进民航领域在网络数字身份、机密计算、隐私保护、数据安全等方向的产业技术创新和应用市场健康发展。

（三）预期的社会效益

本标准编制过程中，在保障安全性的前提下，遵循目前最新发布的密码相关国家标准、行业标准及本领域内的通行做法，可有效规范当前及未来一段时间内民航领域的密码应用，为相关上下游产业单位、信息系统管理部门和测评机构等提供标准支撑，促进整个商用密码产业规范化发展，保障民航领域密码合规应用，维护民航领域相关业务系统信息安全，为谱写交通强国民航新篇章保驾护航。

五、采用国际标准和国外先进标准的程度以及与国际、国外同类标准水平的对比情况

目前，ANSI、AGA、NIST、CPNI、IEC、ISO、IEEE、ISA、NEPC等组织和机构相继提出了一些信息系统安全标准和指南。经查询，可见的专门针对系统密码安全技术的标准比较少，一些国际标准一部分聚焦在网络及信息安全领域，并不单独面向密码技术应用；另一部分针对密码算法和密码技术层面，不针对具体的行业属性进行密码应用整体设计，不具备面向交通或民航领域的体系化密码应用相关标准规范。

相关性较强的标准主要集中在工业控制系统的信息安全防护方面，包括《NIST SP 800-82 工业控制系统信息安全指南》《IEC 62351 数据和通信安全》《ISA/IEC 62443 工业测量和控制过程网络和系统安全》、美国国家标准学会（ANSI）ISA-99系列、《NERC Security Guidelines - Security Guidelines for the Electricity Sector》等，但这些标准关注系统密码应用的内容较少且缺乏系统性描述。

本标准主要对标《信息安全技术 信息系统密码应用基本要求》（GB/T 39786—2021）等有关国家标准，标准中所要求的SM2数字签名算法、SM3密码杂凑算法、祖冲之（ZUC）序列密码算法、SM4分组密码算法、SM9标识密码算法均已正式发布为ISO/IEC国际标准。因此，本标准与

上述国际标准能够保持良好的一致性，不存在版权等知识产权问题。

六、与有关的现行法律、行政法规、民航规章、国家标准和行业标准的关系

我国已在《中华人民共和国密码法》《中华人民共和国网络安全法》《商用密码管理条例》《关键信息基础设施安全保护条例》等法律法规中明确了商用密码应用要求，也发布了《信息安全技术　信息系统密码应用基本要求》（GB/T 39786—2021）、《信息安全技术　密码模块安全要求》（GB/T 37092—2018）等国家标准，《关键信息基础设施密码应用要求》（GM/T 0133—2024）等行业标准。

本标准立足于贯彻落实上述国家法律法规、标准规范并保持内容一致，涉及的商用密码应用基本要求和增强要求分别针对GB/T 39786—2021的第三级密码应用基本要求和第四级密码应用基本要求进行细化和增强，完全覆盖并满足其提出的要求，并新增部分要求。

本标准与MH/T 0076－2020相辅相成，建立完善民用航空重要网络和信息系统商用密码应用体系。

七、重大不同意见的处理和依据

无。

八、贯彻标准的要求和措施建议（包括组织措施、技术措施、过渡办法等）

1．建议本标准发布实施后，作为指导民用航空领域网络安全保护等级为三级及以上的网络和信息系统、关键信息基础设施的商用密码应用规划、建设、运行及安全性评估的依据，也可供民用航空重要信息系统密码应用的设计、测评、监管等相关方参考。

2．建议本标准发布实施后，行业标准化管理单位加强标准宣贯，有效发挥本标准对实际工作的指导作用。

3．建议本标准发布实施后，民航局配套出台相应管理文件，提高本标准的执行效力。

九、废止现行有关标准的建议

无。

十、重要内容的解释和其他应说明的事项

无。