面向数据要素流通的商用密码安全保障体系研究

黄晶晶[1,2]，田涵宇[1,2]，刘昕宇[1,2]，蔡一鸣[1]，周睿康[1]，李琳[1]，朱峰[1*]

（1. 中国电子技术标准化研究院，北京 100007；
2. 北京赛西科技发展有限责任公司，北京 100176）

摘要：随着可信数据空间发展行动计划的出台，推动数据要素交易与流通已上升为国家战略。密码技术作为网络安全的核心技术与基础支撑，具备的机密性、完整性、真实性与不可否认性特征，为可信数据空间的数据安全提供了有力支撑。基于此，本文聚焦数据要素流通场景，从技术赋能、标准衔接、管理协同 3 个维度构建商用密码安全保障体系；通过梳理数据全生命周期安全应用需求，提出分层解耦的密码应用架构，搭建覆盖基础通用到应用测评的标准体系，建立兼具制度规范、监督评价与政策协同的综合管理机制。经与传统数据安全及密码应用体系对比分析，该体系在数据业务与密码功能融合深度、全链路安全防护、标准管理协同层面具备显著优势，能够为数据要素安全高效流通提供理论参考与实践路径。

关键词：可信数据空间；数据安全；数据要素流通；密码技术

中图分类号：TP309.2；TP393.08　　**文献标志码：**A

DOI: 10.20172/j.issn.2097-3136.260528

Research on commercial cryptography security assurance system for data element circulation

Huang Jingjing[1,2], Tian Hanyu[1,2], Liu Xinyu[1,2], Cai Yiming[1], Zhou Ruikang[1], Li Lin[1], Zhu Feng[1*]

（1. China Electronics Standardization Institute, Beijing 100007, China；
2. .Beijing CESI Technology Co., Ltd., Beijing 100176, China）

Abstract: With the introduction of the action plan for the development of trusted data space, advancing the transaction and circulation of data elements has become a national strategy. As the core technology and fundamental support of network security, cryptographic technology possesses the characteristics of confidentiality, integrity, authenticity and non-repudiation, which strongly supports data security in trusted data space. Focusing on the scenario of data element circulation, this paper constructs a commercial cryptography security assurance system from three dimensions of technology empowerment, standard alignment and management synergy. By sorting out the security application requirements in the whole life cycle of data, this paper proposes a layered and decoupled cryptographic application framework, establishes a standard system covering general basic specifications to application evaluation, and builds a comprehensive management mechanism integrating institutional norms, supervision and evaluation, as well as policy coordination. Comparative analysis with traditional data security and cryptographic application systems shows that the proposed system has significant advantages in the integration depth of data business and cryptographic functions, full-link security protection, and the coordination of standards and management, which provides a theoretical reference and practical path for the secure and efficient circulation of data elements.

Keywords: trusted data space; data security; data element circulation; cryptographic technology

* **通信作者：**E-mail: gygfeng@126.com

引用格式：黄晶晶，田涵宇，刘昕宇，等. 面向数据要素流通的商用密码安全保障体系研究 [J]. 网络空间安全科学学报，2026，4（3）：2 - 12.

Citation Format: Huang J J，Tian H Y，Liu X Y，et al. Research on commercial cryptography security assurance system for data element circulation[J]. Journal of Cybersecurity，2026，4（3）：2 - 12.

0　引言

在数字经济成为全球竞争新赛道的背景下，数据作为关键生产要素，其高效流通与安全利用不仅是衡量国家数字竞争力的核心指标，更是推动产业升级、优化资源配置、激发经济潜力的重要支撑[1-2]。党的二十大明确提出“加快建设数字中国”，《中共中央关于制定国民经济和社会发展第十五个五年规划的建议》明确提出“建设开放共享安全的全国一体化数据市场”“建设和运营国家数据基础设施，实施可信数据空间发展行动计划”，将数据要素发展与流通建设提升至国家战略高度[3]。在此背景下，国家发展改革委、国家数据局等部门联合印发《关于完善数据流通安全治理 更好促进数据要素市场化、价值化的实施方案》，明确将“安全贯穿数据供给、流通、使用全过程”列为数据流通治理的核心要求，为数据要素市场的规范发展指明了方向[4]。

因此，从数据要素流通的本质需求出发，构建与数据要素流通相匹配的全链路安全保障体系[5-6]，既是落实国家战略部署的必然要求，也是推动数字经济高质量发展的关键任务。

1　数据要素流通面临的安全问题和挑战

数据要素市场化配置离不开安全、可信的流通环境，商用密码作为保障数据安全的核心技术手段[7]，在数据全生命周期安全防护中发挥着不可替代的重要作用[8-10]。然而，随着数据流通规模不断扩大、场景日益复杂、参与主体更加多元，商用密码在数据流通中的应用面临诸多亟待解决的问题。

首先，数据流通全流程密码体系化应用覆盖不足。当前，商用密码应用多集中于数据传输[11]与存储环节[12]，在数据采集、汇聚、处理、交易、销毁等关键环节存在应用短板，形成数据流通的“安全断点”。例如，在数据采集阶段，部分数据采集工具缺乏有效的密码保护机制，导致原始数据在采集过程中存在被篡改、窃取的风险[13-14]；在数据交易环节，由于行业尚未形成统一的密码应用规范，数据交易双方的身份可信认证、合法权益保障等问题难以有效解决，大幅降低了数据交易的可信度与规范性[15-16]。

其次，数据标准体系与商用密码标准体系协同衔接不足。数据领域标准[17-18]与商用密码标准[19-20]分属不同体系，两类标准在核心要求、适用范围等方面存在交叉重叠与规范空白，导致数据场景下的密码应用缺乏统一的执行依据与管理准则。例如，部分数据标准仅对数据格式、质量等提出要求，未明确对应的密码保护措施，而商用密码标准又未充分考虑数据流通的场景特性，难以适应数据流通中动态变化的安全风险，在数据跨域共享过程中，难以根据数据动态流转状态实时调整密码保护策略，最终造成密码应用与数据业务场景脱节。

此外，不同行业与应用场景的数据在敏感度、流通需求及安全防护要求上存在显著差异。例如，医疗数据涉及公民个人隐私，对数据机密性要求极高[21]；政务数据关系到公共利益和国家安全，需要严格的访问控制和操作追溯机制[22]；工业数据与生产运营密切相关，对数据完整性和实时性要求较高[23]。通用型密码标准难以适配差异化场景安全需求，无法有效指导各行业数据安全应用体系建设。

最后，数据流通领域密码应用管理体系尚不健全。《中华人民共和国密码法》《商用密码管理条例》等法律法规虽为商用密码规范化应用提供了基础制度支撑[24]，但面向数据流通专属场景的专项管理规范仍存在空白，在密码应用推广激励、安全责任划分、跨部门协同监管等方面缺乏明确规定。例如，部分企业因部署成本较高、配套政策激励不足，开展数据流通密码应用建设的积极性较低；跨区域、跨行业的数据流通中，密码应用的监管责任不清晰，导致安全问题难以有效追溯和处置。

上述问题与挑战，严重制约了商用密码在数据要素流通场景的落地应用，阻碍了数据安全流通与合规使用。数据流通安全保障能力的缺失，不仅易引发数据泄露、篡改、滥用等安全风险，还会降低数据要素市场化配置效率，制约数字经济高质量发展。“可信数据空间”作为落实党的二十大“数字中国、网络强国”战略的具体抓手，是实现数据要素流通的具体形态和新型基础设施，也是解决大数据产业“数据孤岛”式困境的重要手段。因此，亟须针对可信数据空间下的数据要素流通场景，开展商用密码安全应用体系研究，构建适配数据供给、流通、使用全流程的密码安全保障体系。

2　可信数据空间数据要素流通的商用密码安全保障体系

可信数据空间是支撑数据与资源共享的数字化新型基础设施，旨在实现不同利益主体间可信、安全、透明的数据共享、交换、流通与交易[25]。可信数据空间是数据要素流通体系的技术保障，能够解

决数据要素提供方、使用方、服务方和监管方等主体间的安全与信任问题[26]。2024 年 11 月 21 日，国家数据局发布《可信数据空间发展行动计划（2024—2028 年）》，明确提出可信数据空间是基于共识规则，实现数据资源共享共用的一种数据流通利用基础设施，是数据要素价值共创的应用生态，是支撑构建全国一体化数据市场的重要载体，并对未来 4 年内可信数据空间的标准体系、技术体系、生态体系和安全体系等方面提出要求，其建设目标为“基本建成广泛互联、资源集聚、生态繁荣、价值共创、治理有序的可信数据空间网络，显著提升各领域数据开发开放与流通使用水平，初步形成与我国经济社会发展水平相适配的数据生态体系”[27]。可信数据空间的建设发展意义重大，是推动数据要素安全流通、释放数据价值的重要支撑，也是未来我国数字经济高质量发展的核心驱动力。

当前，业内保障数据要素流通安全的主流方案存在明显短板：一是通过逐点部署密码设备开展安全防护，缺乏全生命周期防护思维，各环节密码应用相互割裂，“木桶效应”凸显；二是沿用传统边界安全模型，仅聚焦内外网数据传输加密，未覆盖数据本体的确权、溯源、细粒度管控等核心安全需求。本文从技术、标准和管理维度入手，研究提出“四横两纵”的数据要素流通的商用密码安全保障体系架构，如图 1 所示。该体系突破传统单点防护模式，将密码能力深度融入数据采集、传输、存储、处理、使用、销毁的全生命周期流程。整体架构遵循“资源解耦—能力封装—服务赋能—业务适配”的建设逻辑：底层为密码基础支撑层，提供核心密码基础能力；密码服务层对底层能力进行封装，输出标准化统一服务接口；流通安全赋能层依托密码服务搭建适配数据流通场景的安全基座；顶层对应数据要素流通全业务环节，架构两侧的标准体系与管理体系，为整体体系的规范化落地与持续迭代演进提供了保障。

2.1 技术体系

数据要素流通商用密码安全保障技术体系的构建，以实现数据“供得出、流得动、用得好、保安全”为核心目标，聚焦数据安全流通与合规使用需求，结合数据全生命周期各阶段的业务特征精准部署密码技术，推动密码功能与数据业务流深度融合，搭建全链路、多层次的立体化安全防护体系。数据流通前置阶段，可依托密码技术完成数据合规采集、权属界定与分类分级定级等基础工作。数据流通运行阶段，需保障数据共享、交易、使用全流程的机密性与完整性，通过密码技术实现交易过程可溯源、数据使用范围可界定、操作行为可管控，重点覆盖数据传输、存储、处理、交换等核心环节。数据流通收尾阶段，可依托密码技术实现全流程溯源、安全问题定位与数据权益保障，同时实现数据生命周期终结后的安全销毁，核心覆盖流通凭证管理、数据销毁核验等关键环节。

2.1.1 数据采集阶段：可信溯源与质量保障

数据采集阶段的安全需求是确保数据来源可信、采集过程可追溯，防范篡改数据流入可信数据空间，

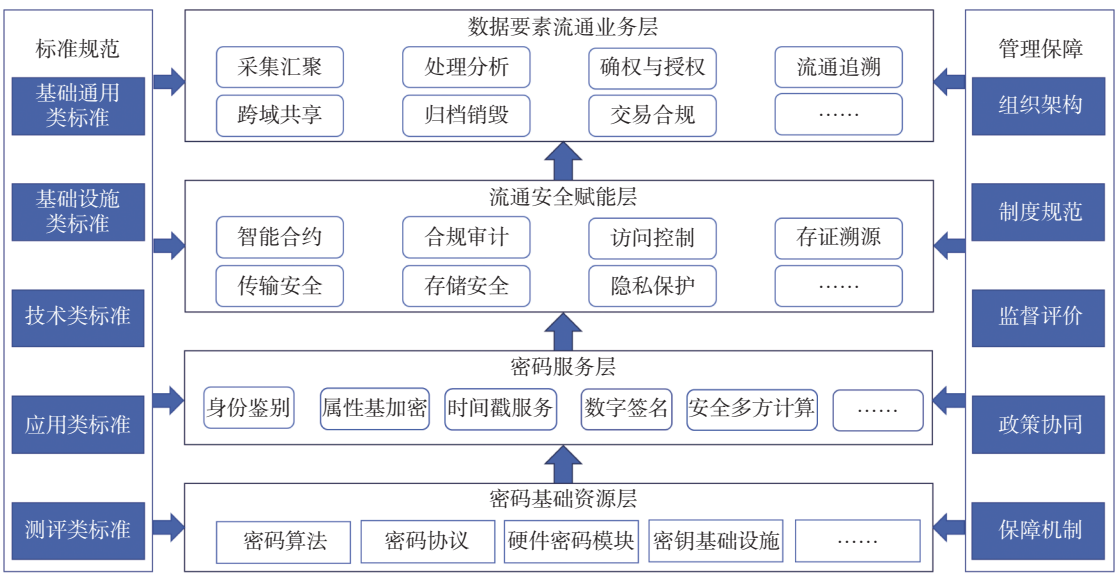

图 1 数据要素流通的商用密码安全保障体系架构

Fig. 1 Commercial cryptography security assurance system architecture for data element circulation

同时保护采集过程中涉及的用户隐私信息。本阶段面临的主要威胁包括：数据采集设备被劫持、数据被篡改、采集主体身份伪造、隐私信息泄露等。

针对上述安全需求，主要采用数字签名、密码杂凑算法、差分隐私等技术满足安全要求，具体实现路径如下。

1）采集主体身份认证：采用 SM2 公钥密码算法的数字证书，对企业、设备、个人等数据采集主体开展身份注册与认证，确保采集主体身份合法、真实有效。数据采集主体在开展数据采集前，需依托数字证书向可信数据空间服务平台发起身份验证请求，由平台完成证书有效性与主体合法性校验，校验通过后才可执行数据采集操作，从而防范非法主体接入采集系统。

2）数据来源溯源：针对采集获取的原始数据，采用 SM3 密码杂凑算法生成数据摘要，结合数字签名技术，由数据采集主体对数据摘要进行签名，将签名信息、采集时间、采集主体信息等元数据与原始数据绑定后上传至可信数据空间服务平台。通过数据摘要校验可验证采集数据未被篡改，而数字签名可实现数据来源可追溯，一旦出现数据安全问题，可快速定位责任采集主体。

数据采集主体也可采用 SM2 数字签名算法对数据权属声明文件进行数字签名，签名信息需包含数据来源、采集时间、权属主体等核心要素，确保权属声明的真实性与不可否认性，依托密码技术实现数据来源真实可溯、交易主体身份真实可信。签名结果需与元数据绑定存储，作为数据交易与监管工作的核心凭证。涉及多主体贡献的数据可采用 SM2 公钥密码算法的门限签名方案[28]实现联合认证，各参与方分别完成签名操作，仅达到预设签名阈值才生成完整确权凭证，保障多方数据权属的公平性与可追溯性。

3）采集数据隐私保护：对于涉及个人隐私、商业机密的用户敏感信息，在采集过程中采用 SM4 分组密码算法实施实时加密，将加密数据上传至可信数据空间服务平台，杜绝原始敏感数据在采集传输链路中发生泄露。面向数据共享与数据分析场景，可采用差分隐私技术添加可控噪声，在保障数据可用性的前提下降低隐私泄露风险。此外，采用属性基加密技术实现细粒度加密访问控制，依据数据分类分级结果配置对应访问属性策略，仅允许满足属性条件的授权主体解密并访问对应级别数据，有效防范越权访问与非法获取行为。

4）采集数据的定价保护：针对数据定价核心指标（如数据规模、数据精度、时效性等），可采用 SM4 分组密码算法对其加密后传输与存储，对应的加密密钥通过 SM2 公钥算法进行加密保护，仅授权定价评估机构通过私钥解密获取相关指标信息，保障数据定价过程的保密性与公正性。

2.1.2　数据传输阶段：可控传输与可信共享

数据传输阶段是可信数据空间实现数据价值释放的核心环节，本阶段安全需求为保障数据传输全程的机密性、完整性与可控性，实现数据“可用不可见、可控可计量”的流通目标，明确数据流通各方权责，保障传输全程可追溯，防范数据在传输链路、交易平台中被窃取、篡改。本阶段面临的主要威胁包括：数据传输窃听与篡改、数据违规转发与滥用、流通主体身份伪造等。

针对上述安全需求，需构建跨部门、跨行业的数据交换密码信任框架，依托商用密码数字证书保障数据交换双方身份可信，通过加密传输通道保障数据交换链路安全，依托数字签名、时间戳服务等技术确保交换数据完整、交换行为不可否认。本阶段主要采用数字签名、区块链存证[29]、安全多方计算[30-31]等技术，具体实现路径如下。

1）数据传输加密：采用商用密码传输层安全协议（TLCP）搭建安全通信环境，基于 SM4 分组密码算法保障传输数据机密性，基于 HMAC-SM3 算法实现数据完整性保护，防范数据在传输过程中被窃听、篡改与伪造。TLCP 通过 SM2 密钥交换协议完成会话密钥安全协商，防范密钥在传输过程中发生泄露。

2）流通主体身份认证与授权：依托商用密码数字证书开展身份认证，对数据提供方、数据使用方、平台运营方等流通主体进行身份校验，确保流通主体身份合法合规。同时，采用属性的访问控制机制[32]结合数字签名技术，对流通主体访问权限实施精细化授权，明确数据使用范围与操作权限，有效防范非法访问与违规转发行为。

3）数据流通追溯与存证：在数据接收、数据使用、数据共享等流通关键节点，生成包含操作时间、操作主体、操作类型、数据标识等信息的追溯凭证。各数据流通主体通过自身 SM2 私钥对凭证进行数字签名，接收方及相关主体可通过对应公钥校验签名有效性，保障凭证来源可信、内容完整。同时，采用区块链存证技术，将流通主体、流通时间、数据摘要、授权范围等关键信息上链存证，实现数据流通过程不可篡改、全程留痕。此外，依托数字签名

技术明确各方权责，一旦出现数据违规流通行为，可依托区块链存证信息快速溯源追责。

4）可控共享与计量：依托智能合约技术[33]，将数据共享协议、收益分配机制转化为可自动执行的规则，基于区块链与密码技术保障合约规则不可篡改，实现数据使用过程的可控性与可计量性。例如，通过数字签名技术验证数据使用方的授权合法性，智能合约完成数据使用行为链上记账与次数统计，实现数据使用可计量、可计费，切实保障数据提供方的合法权益。

2.1.3 数据存储阶段：机密性与完整性保护

数据存储阶段的安全需求是保障数据存储全程的机密性、完整性与可用性，防止数据被非法访问、篡改、泄露或丢失[34]。本阶段面临的主要威胁包括：存储设备被入侵、数据被窃取或篡改等。

针对上述安全需求，需构建分级分布式加密存储体系，依托商用密码技术对静态数据实施细粒度加密与透明加密，确保未授权主体无法读取数据明文，同时结合密钥管理系统实现密钥全生命周期合规管控，具体实现路径如下。

1）数据分级分布式加密存储：根据数据分类分级结果制定差异化加密防护策略，对核心数据实施全量加密存储，密钥由可信密钥管理系统统一管控；对重要数据采用文件级、字段级精准加密，兼顾存储安全性与运行效率。同时，采用 SM2 公钥加密算法对对称加密密钥进行加密保护，防范密钥泄露风险。此外，将数据分片存储至多个节点并分别加密，即便部分节点被非法攻破，攻击者也无法获取完整的核心数据。

2）数据完整性校验：采用基于对称密码算法或密码杂凑算法的消息鉴别码机制、数字签名技术，对存储数据实施全方位完整性保护。一旦监测到数据篡改行为，可及时触发预警并启动对应应急处置方案。对于需存证的核心数据，可结合区块链技术强化全流程安全防护。采用 SM2 公钥密码算法的数字签名技术开展完整性保护时，可同步实现数据真实性与抗抵赖性的多重安全防护。

3）存储设备的安全防护：依托可信执行环境、硬件安全模块构建硬件级安全隔离区域，用于加密密钥等敏感信息的安全存储，防范重要涉密信息被非法窃取。同时，对存储设备接入与访问行为实施严格身份认证，结合数字签名技术完成主体身份校验，依托用户权限体系开展细粒度访问控制，仅认证通过的授权主体可访问存储数据，有效规避非法访问风险。

4）数据备份加密：对存量重要数据开展备份操作时，对备份数据同步落实加密防护，采用与原始数据一致的加密策略，保障备份数据机密性。备份密钥与原始数据密钥实行分离存储，并采用 SM2 公钥加密算法对备份密钥进行加密保护，规避密钥集中泄露引发的批量数据安全风险。

2.1.4 数据处理阶段：隐私保护与合规处理

数据处理阶段的安全需求为保障数据清洗、转换、整合、分析等全流程的隐私安全，防范敏感数据泄露，保障处理后数据的完整性与准确性，契合行业合规管理要求。本阶段主要安全威胁包括：核心与重要敏感数据处理泄露、数据处理结果被篡改、数据处理操作不合规。

针对上述安全需求，可采用安全多方计算、同态加密[35]、可信执行环境等技术，保障数据全程处于加密状态或仅在可信隔离环境内完成运算，规避数据被处理方窃取、泄露的安全风险。同时，依托商用密码算法对计算任务调用、数据处理过程及处理结果进行数字签名，结合安全审计日志，实现数据处理行为可追溯、可审计，保障操作行为不可篡改、不可抵赖，具体实现路径如下。

1）重要数据隐私计算处理：针对多源异构重要数据联合分析场景，采用联邦学习技术实现“数据不出域、模型共训练”。各数据提供方仅在本地完成数据处理与模型迭代，仅上传加密后的模型参数至协同训练节点，依托加密传输机制保障参数交互安全。对于需开展密态计算的业务场景，采用同态加密技术，在不解密原始数据的前提下完成密文直接运算，在满足数据处理业务需求的同时，严格保障数据隐私安全。

2）数据处理追溯：依托 SM2 数字签名算法等商用密码算法，对数据处理主体、处理时间、处理操作、处理结果等关键信息进行签名固化，生成标准化处理日志并上传至可信数据空间服务平台。同时，采用对称密码算法或密码杂凑算法的消息鉴别码机制对处理日志进行完整性保护，保障日志文件不可篡改，实现数据处理全流程可追溯，支撑合规审计与问题溯源工作。

3）数据脱敏安全保障：针对业务敏感数据，采用泛化、随机化、抑制、扰动等脱敏技术，实现敏感信息脱敏屏蔽与隐私安全加固。针对高敏感数据，通过差分隐私技术添加可控噪声，强化隐私保护能力，确保无法通过处理后数据反推原始敏感信息。

同时，对脱敏过程中产生的中间数据、临时数据，采用 SM4 分组密码算法加密保护，杜绝处理环节数据泄露问题。

4）数据安全访问控制：面向共享数据、交易数据等流通数据，采用属性基加密等密码技术，结合角色权限与属性权限双重策略实施细粒度访问控制，严格限定数据使用范围与操作权限，确保仅授权主体可访问对应数据资源。

2.1.5　数据使用阶段：权限管控与违规追溯

数据使用阶段的安全需求为保障数据使用合规性与过程可控性，防范数据违规滥用与信息泄露，实现使用行为全程可追溯、可审计，同时保障数据使用过程的完整性与可用性。本阶段面临的主要威胁包括：数据使用方越权使用数据、数据信息泄露、操作行为违规、数据使用结果被篡改。

针对上述安全需求，本文采用数字签名、访问控制、密码杂凑算法、可信执行环境等技术予以防护，具体实现路径如下。

1）细粒度访问控制：基于 SM2 公钥密码算法数字证书构建精细化访问控制机制，结合数据安全等级、业务应用场景与用户权限维度，对数据使用行为实施严格管控。例如，针对核心数据，仅允许具备对应权限的用户在指定业务场景下使用，且全程开展身份校验，有效规避越权使用风险。

2）数据使用行为追溯：采用 SM2 数字签名算法的数字签名技术，对数据使用过程中的查询、下载、分析、修改等操作进行签名，记录使用主体、操作时间、操作类型、使用结果等关键信息，生成标准化使用日志。同时，采用对称密码算法或密码杂凑算法的消息鉴别码机制对使用日志实施完整性固化，实现数据使用全链条可追溯，支撑合规审计与行为核查工作。

3）使用过程隐私保护：针对核心及重要数据，依托可信执行环境构建硬件隔离的安全执行区间，保障数据在可信可控环境内完成使用，杜绝原始数据泄露。同时依托同态加密技术实现数据密态计算，从根源上规避数据使用过程中的窃取、泄露风险。

4）使用结果合规校验：针对数据使用结果，采用 SM3 密码杂凑算法生成数据摘要，主体基于 SM2 公钥密码算法数字签名，保障数据使用结果的真实性、完整性与不可否认性。

2.1.6　数据归档阶段：长期安全与可追溯

数据归档阶段的安全需求是确保归档数据的长期安全性、完整性与可用性，防范数据被篡改、泄露及丢失，满足合规审计要求并实现归档数据全程可追溯。本阶段面临的主要威胁包括：归档数据被篡改、归档密钥泄露、归档数据被非法访问。

针对上述安全需求，可采用对称加密、非对称加密、密码杂凑算法、区块链存证等技术构建防护机制，具体实现路径如下。

1）归档数据加密存储：采用 SM4 分组密码算法对归档数据实施加密存储，密钥由可信密钥管理系统统一管控并定期迭代更新，防范密钥泄露风险。同时，采用 SM2 公钥加密算法对归档密钥进行加密保护，全方位保障密钥体系安全。

2）归档数据完整性校验：基于对称密码算法或密码杂凑算法的消息鉴别码机制、数字签名技术，对归档数据实施全方位完整性保护。针对需存证的归档数据，可结合区块链技术将数据摘要上链存证，支持归档数据完整性长效核验，满足长期合规审计要求。

2.1.7　数据销毁阶段：彻底清除与合规验证

数据销毁分为物理销毁与逻辑销毁两类，本阶段安全需求为保障数据被彻底安全清除且不可恢复，契合相关法律法规要求，同时实现销毁全过程可追溯、可审计。本阶段面临的主要威胁包括：数据销毁不彻底、销毁记录被篡改、销毁操作不合规。

针对上述安全需求，需依据数据分类分级结果建立标准化数据销毁策略与管理制度，明确销毁场景、销毁对象、销毁方式及合规要求，依托密码杂凑算法、数字签名、密钥销毁等技术实现安全销毁，具体实现路径如下。

1）数据彻底销毁：采用 SM4 分组密码算法加密存储的敏感数据需彻底销毁时，可通过存储介质安全擦除、多轮数据覆写的方式物理清除密文；也可直接销毁数据加密密钥，使密文无法解密，实现合规逻辑销毁。

2）销毁过程追溯与审计：采用 SM2 数字签名算法的商用密码签名技术，对销毁主体、销毁时间、销毁方式、销毁数据清单等信息进行签名固化，生成合规销毁日志。同时，基于对称密码算法或密码杂凑算法的消息鉴别码机制对销毁日志进行完整性保护，保障销毁全程可追溯、可核验，满足合规审计要求。

2.2　标准体系

现行商用密码安全标准中涉及数据安全的规范内容，主要从网络通信、应用数据安全层面针对通用信息系统重要数据的传输与存储环节提出密码应

用要求，但对数据要素流通核心业务环节的覆盖仍存在短板，尤其缺乏与数据确权、数据资源定价、数据流通交易等场景深度耦合的专项密码应用规范。因此，本文以数据流通全生命周期为主线，按照流通前置、流通过程、流通后置全阶段制定差异化密码应用规范，将密码安全要求贯穿数据要素流通全过程。基于此，数据要素流通商用密码安全保障标准体系框架，需覆盖基础概念、设施能力、技术规范、行业应用、测试评估全维度，形成系统化、可落地、可推广的标准架构。

2.2.1 基础通用类标准

建立覆盖数据领域的商用密码相关术语、定义、分类、参考模型和总体框架等通用性标准，为后续标准研制提供统一语言体系和术语规范，保障各类数据要素、流通主体、密码服务能力在跨地域、跨行业场景下保持统一规范、兼容适配，为数据要素流通的密码应用提供统一的顶层设计依据。

2.2.2 基础设施类标准

重点围绕数据存储设施、计算设施、网络设施、流通利用支撑设施，构建适配的密码能力标准与接口规范，明确数据中心、算力平台、数据交换平台等关键基础设施的密码应用配置要求、安全接口调用规范、密钥管理机制与可扩展密码服务框架。通过统一基础设施在身份认证、加解密、签名验签、密钥托管等环节的密码服务接口规范，保障各类流通平台在数据要素市场环境下安全互联互通。

2.2.3 技术类标准

围绕数据采集、汇聚、处理、流通、应用、运营监测、销毁等全生命周期环节，制定覆盖商用密码算法应用、数据最小可用性保护、可信计算、隐私增强技术、数据资产防护、跨域流通安全控制等方向的技术标准，推动数据业务、安全技术与商用密码能力的深度融合与协同适配。

2.2.4 应用类标准

结合可信数据空间典型领域与多样化业务场景，制定场景化商用密码应用专项规范。例如，面向数据流通场景的身份认证与访问控制要求；面向数据交易场景的签名验签与全程可审计要求；面向数据共享场景的最小权限管控与分类分级保护要求等。通过制定场景化、可验证、可落地的商用密码应用标准，明确不同业务场景下数据要素的安全基线与合规边界，有效提升数据交易与数据服务的可信安全水平。

2.2.5 测评类标准

安全测评是落实数据流通全生命周期安全管控的重要手段[36]，需建立覆盖数据采集、使用、交换、处理等关键环节的商用密码应用安全测评标准体系。测评标准需明确测评对象、测评指标、测评实施流程与结果判定规则，其中，测评对象涵盖流通平台、业务系统、服务接口、业务流程等，测评指标包含密码算法合规性、密码技术应用有效性、密码产品合规性、密钥管理规范性等核心维度。

在测评对象遴选层面，需结合数据安全等级、价值属性与应用场景，聚焦数据全生命周期核心测评节点。

在测评实施阶段，可综合采用访谈调研、文档审查、实地核查、工具测试、配置核验、代码审计、渗透测试、回归测试以及基于密码机制的主动分析等多种方式，对数据密码应用合规性进行全方位验证。

在结果判定环节，需依据测评指标完成各对象单项评分，结合各模块关联关系开展综合风险研判，科学判定整体密码安全防护水平，为数据全生命周期商用密码应用能力评估提供客观依据。

2.3 管理体系

数据要素流通商用密码安全管理体系的构建，需聚焦商用密码应用全流程的组织管理、监督考核、效果评估与持续迭代机制，依托制度化、规范化管理方式，保障密码应用在可信数据空间复杂生态中规范、有序、高效落地。该体系核心是搭建涵盖组织架构、制度规范、监督评价、政策协同的一体化管理框架，实现密码应用全流程闭环管理与责任落地。

首先，明确管理组织架构与职责分工，建立跨部门、跨层级协同管理机制，厘清国家主管部门、地方监管机构、平台运营主体、数据供需方、密码服务提供商等各类角色的职责边界与协作机制，构建权责清晰、联动高效的组织保障体系。

其次，在制度规范层面，建立覆盖密码应用全流程的管理制度与标准规程。具体包括：制定密码应用分类分级管理规范，明确不同安全等级数据的密码应用管控要求；建立密钥管理、身份认证、访问控制等专项管理制度，规范各参与主体的操作行为与权责边界；完善密码应用安全审计与日志管理机制，保障操作全程可追溯、责任可界定。

再次，监督评价是管理体系的核心闭环环节，可通过搭建多维度、可量化的密码应用评价体系，实现对密码应用管控状态的常态化监测与周期性评估。该机制不仅保障密码应用合规落地，更聚焦管理措施的执行效能与落地质量，驱动管理体系持续迭代优化和动态完善。

最后，管理体系强调政策协同与配套保障，推动商用密码管理要求与可信数据空间现有政策体系深度融合。研究制定商用密码应用推广的激励与约束机制，明确配套政策支撑方向，为密码管理体系落地实施提供制度保障与资源支撑，确保商用密码技术在可信数据空间场景中合规、精准、高效应用。

2.4　安全保障体系分析

本文所提商用密码安全保障体系立足数据要素流通全过程视角，构建技术、标准、管理三位一体的协同保障机制，摒弃传统单纯的密码技术、设备堆砌与“断点式”防护模式，本文将该体系与传统商用密码应用体系、传统数据安全通用体系进行对比，结果如表 1 所示。

数据要素流通的商用密码安全保障体系的创新性主要体现在以下 3 方面。

1）架构创新：打破传统“密码设施—安全基座—应用”的层级防护模式，提出“资源—服务—赋能—业务”4 层分层架构，通过增设中间层级实现密码功能与业务应用解耦，避免数据流通业务与特定密码产品深度绑定，杜绝因设备更替、算法升级引发的系统大规模改造问题，有效解决了密码功能无法弹性调度的工程应用痛点。

2）标准管理协同创新：构建“技术架构贯通、标准管理贯穿”的一体化保障体系，有效解决数据要素流通场景下密码应用专项标准缺失、配套管理保障制度不完善的行业痛点，推动数据标准与密码标准有效衔接，完善优化配套组织保障体系。

3）动态适配创新：以顶层业务需求牵引密码策略动态适配，支持跨域数据流通场景下，依据数据分类分级结果与安全等级自动匹配加密强度与访问控制粒度，实现安全防护从“静态固化”向“动态自适应”迭代升级，达成密码能力按需调用、全局联动的防护效果。

综上，本体系形成双向闭环运行逻辑：自底向上，基础密码资源经服务层封装、赋能层转化，形成可插拔的标准化安全服务，逐级支撑顶层数据流通业务开展；自顶向下，数据流通全阶段的安全需求与合规要求逐层传导，动态驱动密码策略实时迭代、资源能力弹性调度。体系横向辅以标准、管理双体系纵向贯穿赋能，保障整体架构可在数据要素流通全链路中实现工程化落地与常态化运行。

3　结束语

本文围绕数据要素流通全生命周期的商用密码应用开展系统性研究，梳理数据各流通阶段的核心安全需求，构建了覆盖技术、标准、管理的一体化商用密码安全保障体系。其中，技术体系作为基础支撑，明确密码技术在数据流通各环节的落地路径；标准体系作为统一规范，提供行业标准化建设依据；管理体系作为长效保障，搭建跨域协同、权责明晰的组织制度机制，全方位支撑数据要素市场安全可信运行。

然而，本文的研究仍存在一定局限性。可信数据空间场景下，数据流通与密码技术的融合适配难度较大。数据要素市场涵盖政务、金融、能源、医疗、通信等多领域业务数据，各类场景在数据格式、流通模式、访问权限、业务实时性等方面存在显著差异，现有技术体系跨场景适配能力有限，严苛的密码防护机制易增加数据处理与传输时延，制约数据要素市场化配置的高效落地。若为保障数据流转效率降低密码应用防护强度，则会加剧数据安全风险，诱发数据泄露、篡改、滥用等安全事故。后续

表 1　3 种体系对比

Table 1　Comparison of three systems

对比内容	传统商用密码应用体系	传统数据安全通用体系	数据要素流通的商用密码安全保障体系
覆盖范围	侧重数据存储/传输的安全与基础密码部署	侧重网络边界防护与静态存储	侧重数据全生命周期防护和跨域流通全链路
业务与密码融合度	以密码为中心，业务适配性弱	泛化适配，无行业差异	业务流内嵌密码功能，按需动态调用
标准协同	遵循密码国标，缺少场景适配	数据标准和密码标准割裂	构建“基础—设施—技术—应用—测评”体系，实现数据流通与密码应用的双向衔接
管理闭环	侧重技术实施，管理机制偏弱	事后审计为主，缺乏密码专项监督	组织—制度—监督—政策联动，保障数据要素流通过程中密码应用持续合规、有效
可落地性	高，但有安全断点	中，缺少统一标准	高，标准配套、管理闭环

研究将重点深化安全保障技术体系与多场景数据流通需求的精准适配，进一步提升数据流通、共享、交易全流程的安全性与可信度，助力数字经济高质量、安全化发展。

参考文献：

[1] 李凤华，李晖，牛犇，等. 数据要素流通与安全的研究范畴与未来发展趋势 [J]. 通信学报，2024，45（5）：1-11.
Li F H，Li H，Niu B，et al. Research category and future development trend of data elements circulation and security[J]. Journal on Communications，2024，45（5）：1-11.

[2] 杨明，冯宏霖，王鑫，等. 数据要素市场研究综述：价值、定价与交易 [J]. 网络与信息安全学报，2024，10（3）：1-19.
Yang M，Feng H L，Wang X，et al. Survey of data factor market：value，pricing，and trading[J]. Journal of Network and Information Security，2024，10（3）：1-19.

[3] 中华人民共和国中央人民政府网. 中共中央关于制定国民经济和社会发展第十五个五年规划的建议 [EB/OL].（2025-10-28） [2026-05-02] https://www.gov.cn/zhengce/202510/content_7046050.htm.
The Central People's Government of the People's Republic of China. Recommendations of the central committee of the communist party of China for formulating the 15th five-year plan for national economic and social development[EB/OL].（2025-10-28）[2026-05-02] https://www.gov.cn/zhengce/202510/content_7046050.htm.

[4] 中华人民共和国国家发展和改革委员会网站. 国家发展改革委等部门印发《关于完善数据流通安全治理 更好促进数据要素市场化价值化的实施方案》的通知 [EB/OL].（2025-01-06） [2026-05-02] https://zfxxgk.ndrc.gov.cn/web/iteminfo.jsp?id=20473.
National Development and Reform Commission of the Peopl's Republic of China. Notice of the National Development and Reform Commission and other departments on issuing the “implementation plan for improving data circulation security governance to better promote marketization and value realization of data elements” [EB/OL].（2025-01-06）[2026-05-02] https://zfxxgk.ndrc.gov.cn/web/iteminfo.jsp?id=20473.

[5] 刘立伟，傅超豪，孙泽堃，等. 数据要素流通全流程隐私关键技术：现状、挑战与展望 [J]. 软件学报，2026，37（1）：301-325.
Liu L W，Fu C H，Sun Z K，et al. Privacy key technologies in whole stages of data circulation：current situation，challenges，and prospects[J]. Journal of Software，2026，37（1）：301-325.

[6] 霍炜，郁昱，杨糠，等. 隐私保护计算密码技术研究进展与应用 [J]. 中国科学:信息科学，2023，53（9）：1688-1733.
Huo W，Yu Y，Yang K，et al. Privacy-preserving cryptographic algorithms and protocols: a survey on designs and applications[J]. Scientia Sinica Informationis，2023，53（9）：1688-1733.

[7] 霍炜，郭启全，马原. 商用密码应用与安全性评估 [M]. 北京：电子工业出版社，2020：2-3.
Huo W，Guo Q Q， Ma Y. Application and security evaluation of commercial cryptography[M]. Beijing： Publishing House of Electronics Industry，2020：2-3.

[8] 范建，胡兴元，刘京，等. 可信数据空间安全防护体系研究 [J]. 中国信息界，2025（8）：109-111.
Fan J，Hu X Y，Liu J，et al. Research on security protection system of trusted data space[J]. Information China，2025（8）：109-111.

[9] 王森，许涛，李金贵. 基于属性加密的数据共享管理研究 [J]. 信息安全研究，2023，9（11）：1061-1066.
Wang S， Xu T， Li J G. Research on data sharing management based on attribute-based encryption[J]. Journal of Information Security Research，2023，9（11）：1061-1066.

[10] 尤玮婧. 数据要素确权中的密码学技术 [J]. 中国计算机学会通讯，2025，21（4）：35-41.
You W J. Cryptographic technologies in data element right confirmation[J]. Communications of the CCF，2025，21（4）：35-41.

[11] 严星宇，赵川，徐雁飞. 券商行业商用密码应用与实践 [J]. 信息安全研究，2023，9（7）：707-712.
Yan X Y，Zhao C，Xu Y F. Application and implementation of commercial cryptographic algorithm in securities industry[J]. Journal of Information Security Research，2023，9（7）：707-712.

[12] 王中武. 商用密码在数据仓库中的应用研究 [J]. 信息安全与通信保密，2025（2）：97-104.
Wang Z W. Research on the application of commercial cryptography in data warehouse[J]. Information Security and Communications Privacy，2025（2）：97-104.

[13] Suliman M，Halimi A，Kadhe S R，et al. Towards a re-evaluation of data forging attacks in practice[C]//34th USENIX Security Symposium （USENIX Security 25）. Seattle：USENIX Association，2025：5505-5524.

[14] Hu J M，Yang X F，Yang L X. A framework for detecting false data injection attacks in large-scale wireless sensor networks[J]. Sensors，2024，24（5）：1643.

[15] Rao Z Y，You L，Hu G R，et al. EBDTS：an efficient BCoT-

based data trading system using PUF for authentication[J]. IEEE Transactions on Network and Service Management，2024，21（5）：5795-5808.

[16] Chen F M，Zhao B，Gao Y L，et al. BTDA：Two-factor dynamic identity authentication scheme for data trading based on alliance chain[J]. The Journal of Supercomputing，2023，79（17）：19118-19137.

[17] 全国数据标准化技术委员会. 可信数据空间技术架构：TC609-6-2025-01[S]，北京：全国数据标准化技术委员会，2025.

National Technical Committee 609 on Data of Standardization Administration of China. Technical architecture of trusted data space：TC609-6-2025-01[S]. Beijing：National Technical Committee 609 on Data of Standardization Administration of China，2025.

[18] 全国数据标准化技术委员会. 可信数据空间使用控制技术要求：TC609-6-2025-15[S]. 北京：全国数据标准化技术委员会，2025.

National Technical Committee 609 on Data of Standardization Administration of China. Technical requirements for usage control of trusted data space：TC609-6-2025-15[S]. Beijing：National Technical Committee 609 on Data of Standardization Administration of China，2025.

[19] 田敏求，夏鲁宁，张众，等. 我国密码行业标准综述（上）[J]. 信息技术与标准化，2019（3）：52-55.

Tian M Q，Xia L N，Zhang Z，et al. Review on Chinese cryptography industry standards（part one）[J]. Information Technology & Standardization，2019（3）：52-55.

[20] 田敏求，夏鲁宁，张众，等. 我国密码行业标准综述（下）[J]. 信息技术与标准化，2019（4）：43-48.

Tian M Q，Xia L N，Zhang Z，et al. Review on Chinese cryptography industry standards（part two）[J]. Information Technology & Standardization，2019（4）：43-48.

[21] 吴龙，杨洋. 商用密码在医院电子病历系统存储加密中的应用 [J]. 中国卫生信息管理杂志，2023，20（5）：715-722，729.

Wu L，Yang Y. Application of domestic commercial password in storage and encryption reform of hospital electronic medical record system[J]. Chinese Journal of Health Informatics and Management，2023，20（5）：715-722，729.

[22] 白荣华，魏强，郭瑞，等. 政务信息系统商用密码集约化平台设计与实现 [J]. 信息安全研究，2023，9（5）：461-468.

Bai R H，Wei Q，Guo R，et al. Design and implementation of cryptography intensive platform for government information system[J]. Journal of Information Security Research，2023，9（5）：461-468.

[23] 姚红云，褚瑞，李红霞，等. 基于国产商用密码的核安保系统解决方案研究 [J]. 自动化仪表，2023，44（S1）：268-271，276.

Yao H Y，Chu R，Li H X，et al. Research on nuclear security system solutions based on domestic commercial passwords[J]. Process Automation Instrumentation，2023，44（S1）：268-271，276.

[24] 国家密码管理局网站. 关键信息基础设施商用密码使用管理规定 [EB/OL].（2025-06-27）[2026-04-10]. https://oscca. gov. cn/sca/xxgk/2025-06/27/content_1061270. shtml.

State Cryptography Administration of China. Provisions on administration of the use of commercial cryptography in critical information infrastructure[EB/OL].（2025-06-27）[2026-04-10]. https://oscca.gov.cn/sca/xxgk/2025-06/27/content_1061270.shtml.

[25] IEEE standard for trusted data matrix system architecture[EB/OL].（2024-12-13）[2026-04-10]. https://ieeexplore. ieee. org/document /10797717.

[26] 杨云龙，张亮，杨旭蕾. 可信数据空间助力数据要素高效流通 [J]. 邮电设计技术，2024（2）：57-61.

Yang Y L，Zhang L，Yang X L. Trusted data space helps efficient circulation of data elements[J]. Designing Techniques of Posts and Telecommunications，2024（2）：57-61.

[27] 国家数据局. 国家数据局关于印发《可信数据空间发展行动计划（2024-2028 年）》的通知 [EB/OL].（2024-11-21）[2026-04-10]. https://www.gov.cn/zhengce/zhengceku/202411/content_6996363.htm.

National Data Administration. Notice of the national data administration on issuing the trusted data space development action plan（2024–2028）[EB/OL].（2024-11-21）[2026-04-10]. https://www.gov.cn/zhengce/zhengceku/202411/content_6996363.htm.

[28] 刘振亚，林璟锵. SM2 数字签名算法的两方门限计算方案框架 [J]. 软件学报，2025，36（5）：2188-2211.

Liu Z Y，Lin J Q. Framework of two-party threshold schemes for SM2 digital signature algorithms[J]. Journal of Software，2025，36（5）：2188-2211.

[29] Thilakavathy P，Jayachitra S，Aeron A，et al. Investigating blockchain security mechanisms for tamper-proof data storage[C]//Proceedings of the 2023 International Conference on Communication，Security and Artificial Intelligence（ICCSAI）. Piscataway：IEEE Press，2023：926-930.

[30] Mohassel P，Zhang Y P. SecureML：a system for scalable privacy-preserving machine learning[C]//Proceedings of the 2017 IEEE Symposium on Security and Privacy（SP）. Piscataway：IEEE Press，2017：19-38.

[31] Zhou I，Tofigh F，Piccardi M，et al. Secure multi-party computation for machine learning：a survey[J]. IEEE Access，2024，12：53881-53899.

[32] 房梁，殷丽华，郭云川，等. 基于属性的访问控制关键技术研究综述 [J]. 计算机学报，2017，40（7）：1680-1698.
Fang L，Yin L H，Guo Y C，et al. A survey of key technologies in attribute-based access control scheme[J]. Chinese Journal of Computers，2017，40（7）：1680-1698.

[33] Steffen S，Bichsel B，Gersbach M，et al. Zkay：specifying and enforcing data privacy in smart contracts[C]//Proceedings of the 2019 ACM SIGSAC Conference on Computer and Communications Security. New York：ACM，2019：1759-1776.

[34] Yang X Y，Luo Q C，Xu J，et al. Data secure storage mechanism for trustworthy data space[J]. Electronics，2025，14（21）：4348.

[35] Gentry C. Fully homomorphic encryption using ideal lattices[C]//Proceedings of the Forty-First Annual ACM Symposium on Theory of Computing. New York：ACM，2009：169-178.

[36] 黄晶晶，孙淑娴，周睿康，等. 商用密码应用安全性评估 [J]. 信息安全与通信保密，2023（3）：113-121.
Huang J J，Sun S X，Zhou R K，et al. Security evaluation of commercial cryptography application[J]. Information Security and Communications Privacy，2023（3）：113-121.