可信数据空间商用密码应用指标体系与测评模型研究

李佳曦[1*]，陈海虹[2]，夏鲁宁[3]
（1. 中国信息通信研究院，北京 100083；
2. 中国科学院大学密码学院，北京 100049；
3. 北京数字认证股份有限公司，北京 100080）

摘要：可信数据空间是基于共识规则连接多方主体、实现数据资源共享共用的数据流通利用基础设施，其以数据要素价值共创为核心应用生态，是构建全国一体化数据市场的重要载体。在此背景下，合规、正确、有效地使用商用密码为可信数据空间构建安全底座，实现数据全生命周期安全防护，已成为可信数据空间发展、数据要素流通利用亟须解决的重要问题。针对可信数据空间分布式架构特征及“集中管控、分布式执行、数据不出域、可用不可见”的核心功能，本文将可信数据空间核心架构解耦，划分成 5 大安全域，并系统分析典型安全风险，梳理全场景密码应用保障要求与测评需求。在此基础上，严格遵循 GB/T 39786—2021 框架，构建适配可信数据空间的商用密码应用指标体系与测评模型，并从理论分析层面验证体系模型的有效性与适用性，该研究为商用密码应用与测评实施提供参考。

关键词：可信数据空间；数据流通利用基础设施；商用密码应用安全性评估；指标体系；安全域
中图分类号：TP309.7 **文献标志码：**A
DOI: 10.20172/j.issn.2097-3136.260610

Research on indicator system and evaluation model for commercial cryptography application in trusted data space

Li Jiaxi[1*], Chen Haihong[2], Xia Luning[3]
（1. China Academy of Information and Communications Technology, Beijing 100083, China；
2. School of Cryptology University of Chinese Academy of Sciences, Beijing 100049, China；
3. Beijing Digital Certification Co., Ltd., Beijing, 100080, China）

Abstract: Trusted data space (TDS) is a data circulation and utilization infrastructure that connects multiple stakeholders and realizes shared use of data resources based on consensus rules. As an application ecology for value co-creation of data elements, it serves as an important carrier to support the construction of a national integrated data market. Against this background, the compliant, correct and effective application of commercial cryptography to build a security foundation for TDS and realize the full life-cycle protection of data has become an urgent issue for the development of TDS and the compliant and efficient circulation of data elements. In view of the distributed federation architecture of trusted data space composed of a central service platform and multiple distributed access nodes, as well as its core functions of "centralized control, distributed execution, data in-domain, and available but invisible", this paper decouples the core architecture of TDS and divides it into five security domains. It systematically analyzes the typical security risks, and sorts out the cryptography application requirements and evaluation demands in full scenarios. On this basis, in strict accordance with the framework of GB/T 39786—2021, an indicator system and evaluation model for the security evaluation of commercial cryptography application adapted to TDS are constructed, and the effectiveness and applicability of the system are verified through theoretical analysis. This

* **通信作者：**E-mail: 674752146@qq.com

引用格式：李佳曦，陈海虹，夏鲁宁. 可信数据空间商用密码应用指标体系与测评模型研究 [J]. 网络空间安全科学学报，2026，4（3）：27 - 41.
Citation Format: Li J X，Chen H H，Xia L N. Research on indicator system and evaluation model for commercial cryptography application in trusted data space[J]. Journal of Cybersecurity，2026，4（3）：27 - 41.

research provides references for the application and evaluation implementation of commercial cryptography.

Keywords: trusted data space; data circulation and utilization infrastructure; security evaluation of commercial cryptography application; indicator system; security domain

0 引言

0.1 研究背景

《中华人民共和国国民经济和社会发展第十五个五年规划纲要》明确建立健全数据产权、流通利用、收益分配、安全治理等数据要素基础制度。完善数据领域法律法规，健全数据采集、存储、流通、使用管理规则。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。实施数据分类分级管理，提升数据安全保护能力等多项要求。国家数据局发布的《可信数据空间发展行动计划（2024—2028 年）》提出发展目标：到 2028 年建成 100 个以上可信数据空间[1]，形成覆盖多领域的可信数据空间网络。在此背景下，可信数据空间作为打破数据孤岛、实现数据“可用不可见、可控可计量”的关键技术，已成为构建数据流通利用基础设施、打造数据要素价值共创生态、建设全国一体化数据市场的重要载体。

商用密码作为网络空间安全的核心技术，能够为可信数据空间搭建身份可信、数据可控、行为可溯的安全底座[2]。在此基础上，商用密码应用安全性评估（以下简称“密评”）能够进一步检验密码应用的合规性、正确性、有效性，为保障数据安全流通提供坚实基础。随着可信数据空间部署建设进度加快，针对可信数据空间的密评体系研究愈发紧迫。与传统信息系统相比，可信数据空间存在安全边界模糊、数据流通主体身份多样、跨域流通导致密钥管理难度提升等挑战[3]，现有通用网络与信息系统的密码应用及评估要求难以适配其密码安全保障需求。因此，亟须面向可信数据空间自身架构及业务逻辑搭建密评指标体系与测评模型。相关研究兼具理论创新价值与工程实践价值。

0.2 国内外研究现状

在可信数据空间及其安全评测领域，国内外已形成部分技术标准与评估方法，但面向商用密码应用的多安全域、分布式场景下的专项测评模型仍未形成成熟方案。

国际上，国际数据空间协会（IDSA）发布的参考架构模型（IDS-RAM v4.0+）及组件认证规范[4]，对数据空间连接器的身份鉴别、传输层加密、数据使用控制提出了明确的密码应用要求[5]，但其认证体系侧重于连接器功能与安全一致性测试，未系统建立密码应用指标体系，无法适配 GB/T 39786—2021[6]。GAIA-X 信任框架强调联邦身份管理与可验证凭证体系[7]，但在密态计算、跨域密钥协同等场景的专项测评指标仍缺乏成的体系支撑。NIST SP 800-53A 提供了通用信息系统的密码控制评估方法（如 SC 系列控制项）[8]，但其针对的是传统单域信息系统，未针对“数据不出域、可用不可见”的分布式数据空间架构进行场景化裁剪与扩展。ISO/IEC 27001:2022 附录 A.8、A.10 等条款对密码控制提出了管理要求[9]，并参照 ISO/IEC 27007 提供审计指南，但该类条款聚焦信息安全管理体系，缺乏面向数据空间业务全流程的技术性密评操作模型。此外，Khan 等[5] 提出的系统理论安全分析方法侧重于工控系统脆弱性识别，未涉及数据空间密码测评指标体系。

国内，商用密码应用安全性评估领域已形成完整标准体系，包含 GB/T 39786—2021《信息安全技术 系统密码应用基本要求》、GB/T 43206—2023《信息安全技术 信息系统密码应用测评要求》两类核心标准。在扩展领域方面，目前已有政务信息系统、云计算平台等场景的密评指导文件，但缺乏针对分布式可信数据空间的专项研究。现有密评体系以“单信任边界、单运营主体”为基础，对多主体接入、跨域数据流转、密态计算环境等数据空间特有场景的测评覆盖不足[10]。

在可信数据空间安全领域，国内外现有研究多聚焦架构设计、身份认证、隐私计算融合、区块链存证等方向，对密码应用仅侧重算法选型、密钥管理方案，尚未形成“安全域划分–风险映射–密码应用–密码测评”的闭环模型。本文在此基础上，面向可信数据空间分布式架构，构建技术、管理双维度测评体系，为跨域密码应用专项评估提供系统性支撑。

1 可信数据空间密码应用安全风险分析

1.1 可信数据空间核心架构

可信数据空间主要由可信数据空间服务平台和接入连接器两大核心部分组成。其中，可信数据空间服务平台是运营方开展数据空间运营的核心载体，

为各参与方提供数据流通、数据使用的基础服务，是实现数据主权保障与可信共享的核心枢纽。接入连接器是各参与方融入可信数据空间生态的唯一入口，数据提供方、使用方、服务方均通过该连接器完成数据提供、使用及增值服务。与此同时，接入连接器也是依据数字合约执行数据使用控制策略的核心系统载体。可信数据空间技术架构[11]如图 1 所示。

1.2　可信数据空间的安全域

可信数据空间架构随着产业发展不断迭代，在考虑安全问题时，可结合其分布式架构、数据流通全流程特性，参考 3GPP 33.501 5G 安全规范[12]，从逻辑层面梳理可信数据空间本体与外围设施，以及跨空间互联通道，抽象划分出接入域、内部网络域、服务域、计算域、外部连通域 5 大安全域[13]。各安全域功能边界清晰、风险类型独立，如图 2 所示。

接入域是指终端用户、管理员、基础设施平台、连接器等参与主体，数据资产、数据产品等流通交易客体，以及算法、合约、安全策略等数据资源，在接入可信数据空间过程中所涉及的安全场景与保护对象集合。

服务域是指用户数据交易所需的监测存证、合约协商、算法调用、使用策略控制、跨连接器数据路由、数据计算等功能所涉及的安全场景与保护对象集合。

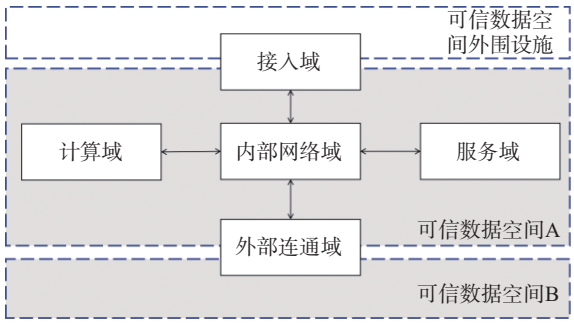

图 2　安全域划分示意

Fig. 2　Schematic of security domain division

内部网络域是指可信数据空间内各通信、存储、计算节点之间，以及富计算节点与机密计算节点之间网络连接所涉及的安全场景与保护对象集合，涵盖服务器内网、云平台虚拟机网络、虚机直通网络等。

计算域是可信数据空间各类安全计算节点所涉及的安全场景与保护对象集合，覆盖机密虚拟机、机密容器、运行环境、安全监控器、底层硬件平台等场景。

外部连通域是指跨主体、跨机构场景下，数据路由策略、跨域会话管理、使用控制策略执行与信任凭证交互过程中所涉及的安全场景与保护对象集合。

安全域本质上是对可信数据空间内的保护对象（及其安全需求）做分类梳理。从商用密码应用视角来看，同一安全域内的保护对象可分属 GB/T 39786—2021 划定的不同安全层面，本文第 4 节构建指标体系与测评模型时，已匹配保护对象在安全层

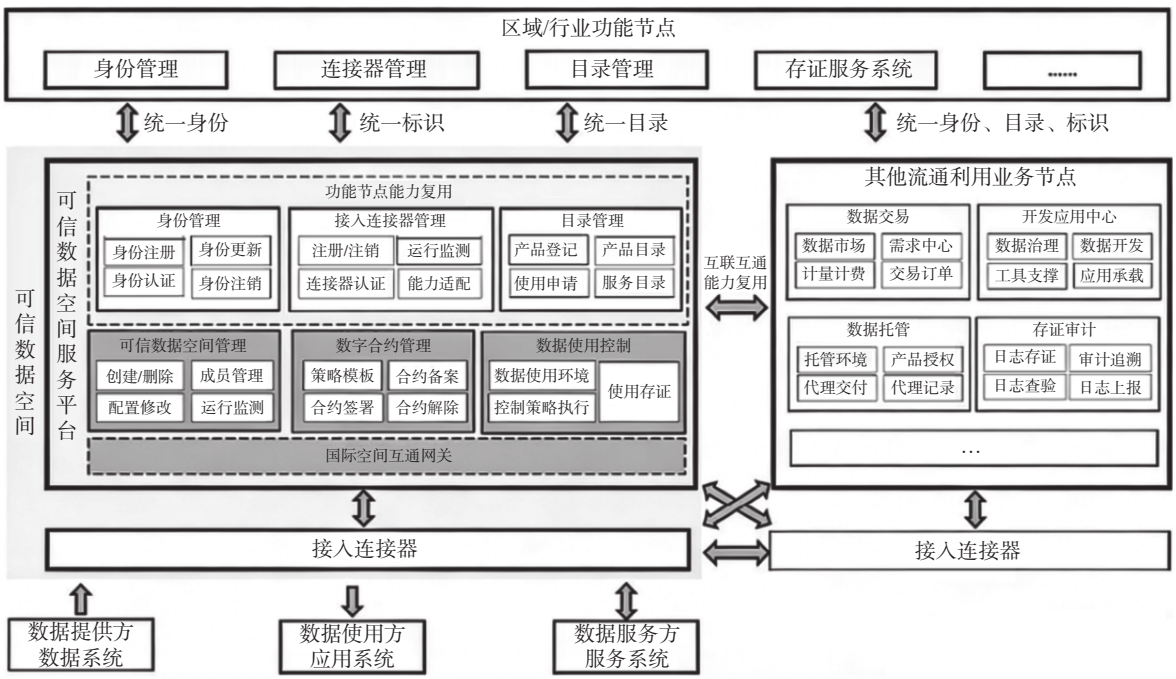

图 1　可信数据空间技术架构

Fig. 1　Technical architecture of trusted data space

面、安全域维度的对应关系。

1.3 安全域典型安全风险分析

接入域：数据提供方、数据使用方通过接入连接器完成身份注册与认证，随后发布数据目录、协商数据合约或执行数据使用控制策略。接入过程涉及用户凭证（如身份证号、手机验证码、数字证书）、接入连接器设备身份及接入链路的合法性验证。若用户凭证在注册、登录或传输过程中被窃取（如通过钓鱼网站、公共网络监听或第三方平台数据泄露），攻击者可利用这些凭证冒用合法用户身份登录接入连接器。更严重的是，若接入连接器仅依赖简单的验证码或静态口令，未启用基于商用密码的多因素认证（SM2 数字证书+动态口令），攻击者可绕过身份核验机制，伪造受信任的参与方节点或替换合法接入设备[14]。身份或设备被冒用后，攻击者可非法发布虚假数据目录、签署或篡改数字合约以窃取高价值数据，越权访问敏感数据资产，甚至植入恶意控制策略干扰其他连接器正常运行[15]。这将直接导致数据资产非法流出、交易合约失效、审计追溯失败，以及数据提供方与使用方之间信任崩塌，进而破坏整个数据空间的合规运营基础，可能引发重大数据泄露风险。

服务域：可信数据空间服务域为用户提供数字合约协商、数据目录查询、使用控制策略分发、运行日志存证等核心功能。这些服务支撑跨参与方业务交互，是数据流通的核心业务中枢。数字合约在协商、签署、存储过程中若未经密码完整性保护，攻击者可篡改合约条款；数据目录查询请求若被劫持，攻击者可伪造目录响应，诱导使用方连接至虚假数据节点；使用控制策略在传输或存储时若被泄露或篡改，可能导致策略绕过；运行日志若被篡改或删除，攻击者可掩盖自身非法操作痕迹。合约篡改会造成数据提供方在非授权范围内提供数据，引发数据资产超范围使用；目录劫持可诱导使用方将敏感数据发送至攻击者控制的节点；策略篡改可使“数据不出域”的控制机制失效，引发数据直接泄露；日志损毁将导致事后无法追溯安全事件责任主体，无法满足合规审计要求。

内部网络域：内部网络域覆盖接入连接器、服务平台、各计算节点间全部通信链路，其主要安全风险如下：通信链路未使用国密 TLCP（transport layer cryptography protocol）建立加密通道时，攻击者可通过流量镜像、ARP（address resolution protocol）欺骗等方式窃听通信报文，获取数据目录、合约内容、使用控制策略等敏感信息，或实施中间人攻击篡改合约参数、计算结果、控制策略；通信节点之间若未采用 SM2 数字证书进行双向身份鉴别，攻击者可伪造连接器或服务平台身份，骗取其他节点信任后窃取或篡改数据；密钥交换协议应用不当时，会话密钥协商过程可能被破解（如算法降级攻击、无效曲线攻击），导致通信内容被解密；远程证明通道若无密码保护，攻击者可拦截或伪造证明报告，使验证方信任已被篡改的机密计算环境。上述风险一旦被利用，将导致数据资产泄露、使用控制约束失效、计算环境不可信，严重时可使整个数据空间的信任基础崩塌。

计算域：可信数据空间的机密计算节点（如可信执行环境（TEE）、机密虚拟机）执行密态计算、多方安全计算、隐私计算等任务，处理多方用户的敏感数据。计算过程涉及输入数据加载、中间结果暂存、计算结果输出以及代码/固件的加载执行。若计算环境未采用密码技术进行隔离保护或远程证明，攻击者可通过伪造、篡改环境配置，使敏感计算在不可信环境中执行，导致多个参与方的原始数据被恢复或泄露；若计算输入、中间结果、输出结果未进行全流程加密，攻击者可利用内存嗅探、侧信道攻击、调试接口遍历等方式窃取计算过程中的明文数据；若可执行程序或固件未进行代码签名验证，攻击者可植入恶意代码，窃取或篡改计算结果，引发如信贷审批、医疗诊断等业务场景决策错误；密码算法使用不当或密钥管理存在漏洞，会使整个计算节点的安全保障能力失效，成为攻击者长期窃取数据的入侵载体。

外部连通域：覆盖不同可信数据空间互联互通、跨域数据交互的场景，是搭建全国一体化数据市场的关键安全边界。其主要安全风险包括：跨域身份伪造与权限映射攻击，攻击者利用跨域信任传递关系，在薄弱接入点伪造身份后渗透到其他数据空间，或利用身份/角色映射配置错误获得超出授权的访问权限；跨域数据传输过程中，若未使用国密安全通信协议，攻击者可窃听或篡改跨域报文，甚至强制降级为弱加密算法；攻击者可利用跨域策略冲突，结合两个数据空间差异化安全规则（如一方允许聚合输出，另一方允许明细查询）组合规避数据使用管控约束；跨域信任链断裂风险（如跨域互认的 CA 证书过期未更新）可能导致跨域通信中断或被攻击者滥用；跨域日志若未采用密码技术保护，攻击者可伪造或篡改日志条目，使跨域安全事件无法追溯。上述风险一旦发生，会引发跨域数据泄露、越权访

问、责任无法追溯，严重阻碍全国一体化数据市场的安全有序运行。

1.4　可信数据空间安全挑战与密码映射分析

与传统信息系统相比，可信数据空间在架构与流通模式上存在 3 大核心挑战，需在密码应用与测评体系中给出应对方案。下文将从安全边界、身份体系、密钥管理 3 个维度逐一拆解安全挑战，并结合可信数据空间的架构特征完成密码应用场景映射。

1）安全边界更加动态模糊。传统系统依赖静态网络分区与物理隔离，而可信数据空间以数据跨域流动为主线，安全边界随数据生命周期（采集、加工、流通、销毁）动态延伸。该特性使防护重心从“网络边界”转向“数据合约与密码凭证”，需在服务域与外部连通域部署动态策略引擎与属性密码，实现“策略随数据流转”。

2）多主体身份异构。数据流通链路涵盖数据提供方、使用方、算力节点、监管审计方等，身份标识涵盖去中心化身份（DID）、个人数字身份、设备指纹、智能合约地址等类型。传统集中式公钥基础设施（PKI）难以支撑高频跨域互认，易引发身份伪造与越权访问，需在接入域构建去中心化身份解析体系与跨域信任锚点，支撑细粒度权限授权与操作行为可追溯。

3）跨域密钥管理复杂。多机构协同使密钥生命周期从“单域闭环”转为“联邦协同”，密钥分发频次、轮换权责、托管归属规则难以统一。传统密钥管理系统（KMS）面临跨域信任链断裂与合规审计断点风险，需在计算域与内部网络域引入门限密钥管理、国密 SM9 标识密码与硬件安全模块（HSM）联邦架构，实现密钥“可用不可见、可管可追溯”。

2　可信数据空间密码应用与测评需求

2.1　可信数据空间密码应用需求

接入域：接入主体需采用密码技术标识真实身份并申领身份凭证（如数字证书）；服务平台、接入连接器需分别采用密码技术标识自身真实身份并配备对应身份凭证；接入连接器需采用密码技术完成接入主体身份鉴别、安全通信链路搭建，并具备访问控制、密钥管理能力。安全域保护对象与密码应用需求如图 3 所示。

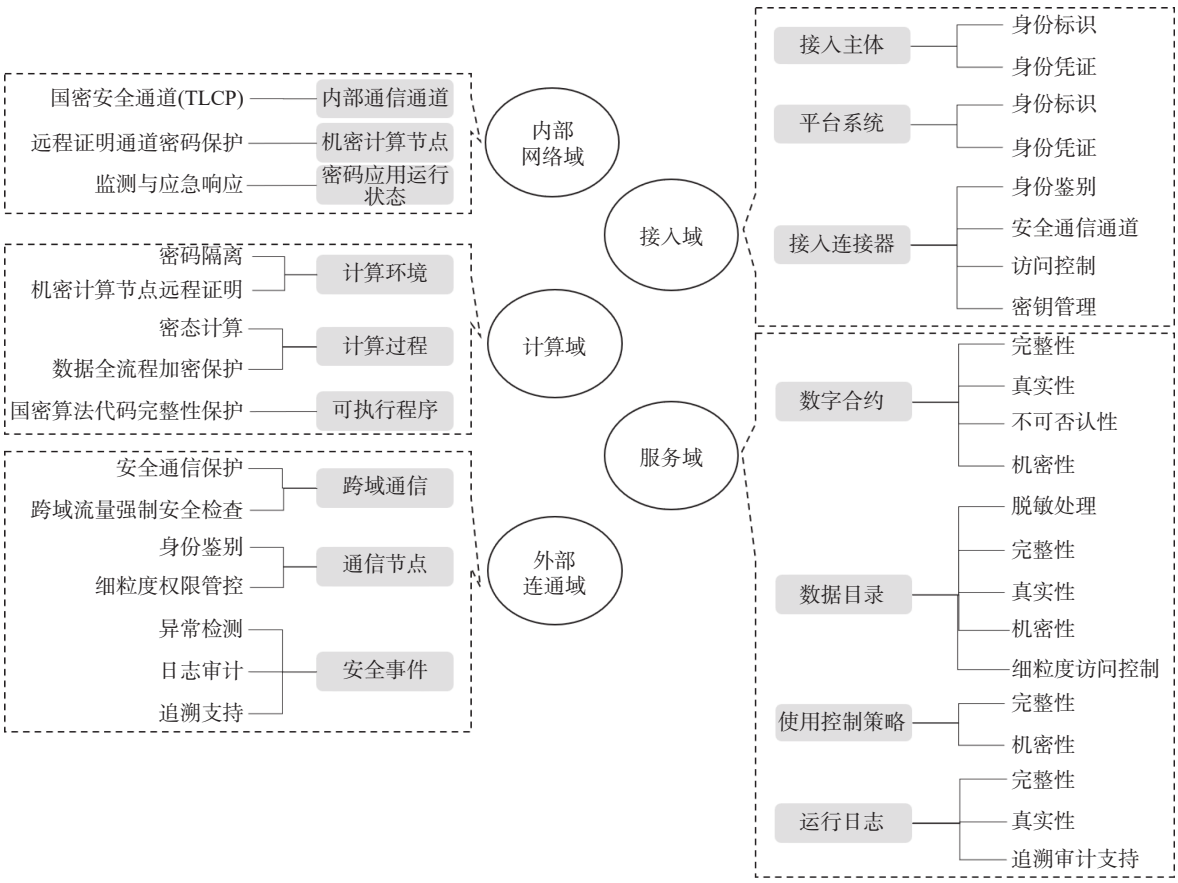

图 3　安全域保护对象与密码应用需求

Fig. 3　Security domain protected objects and cryptographic application requirements

服务域：数字合约采用密码技术实现完整性、真实性、不可否认性保护，按需开展机密性保护；数据目录采用密码技术实现脱敏、完整性、真实性与机密性保护，并配套细粒度访问控制；使用控制策略采用密码技术实现完整性保护，按需开展机密性保护；运行日志采用密码技术实现真实性、完整性保护，支撑事后追溯审计。

内部网络域：采用密码技术构建安全通信链路，如部署 TLCP；依托密码技术保护机密计算节点远程证明链路；开展密码应用常态化监测与应急响应。

计算域：依托密码技术实现计算环境隔离防护与机密计算节点远程证明；基于密态计算完成计算全流程数据加密保护；采用商用密码算法防护可执行程序，保障代码完整可信。

外部连通域：采用密码技术实现跨域安全通信与跨域流量强制安全检查，完成跨域通信节点身份鉴别与细粒度权限管控；同步配套异常检测与日志审计能力，支撑跨域安全事件追溯。

2.2 可信数据空间密码测评需求

本文搭建覆盖可信数据空间逻辑层与底层基础设施的密评框架，既兼容 GB/T 39786—2021、GB/T 43206—2023[16] 通用密码应用测评框架（覆盖标准划定的各层级测评对象），又结合各安全域风险应对需求，对身份认证、跨域密钥管理、密态计算[17]、跨域连通等特有场景设计专项测评项，优化通用密评指标在可信数据空间场景下的适配能力。

2.2.1 接入域

接入域面向可信数据空间接入节点、连接器、边界防护设备，重点覆盖接入认证、边界防护、设备安全、数据云存储安全等场景。专用测评项包括以下内容。

物理和环境安全：核查接入节点机房密码门禁部署效果、机房监控视频密码保护合规程度、机房操作日志完整保护能力。

网络和通信安全：核验商用密码网关部署、接入节点边界身份认证、接入链路加密通道搭建、边界隐写数据过滤、加密通道定期安全检测的能力。

设备和计算安全：核验接入节点设备登录身份鉴别、设备固件完整性保护、设备计算环境隔离与访问控制、设备操作日志加密存证、远程管理通道加密能力。

应用和数据安全：核验接入主体身份鉴别、接入数据加密传输与授权解密、数据标签完整性保护、数据使用可追溯保障能力。

2.2.2 内部网络域

内部网络域面向可信数据空间内部网络和网络设备，重点覆盖内部网络通信安全、网络节点设备安全的场景。专用测评项包括以下内容。

物理和环境安全：核验网络设备机房密码门禁部署、网络设备物理防非法接入阻断、网络设备操作日志加密与完整性保护措施。

网络和通信安全：对存在通信交互的内部节点（网络节点、计算节点、存储节点等）开展身份鉴别，核验网络报文加密、安全通道实时监测能力。

设备和计算安全：核验网络设备管理员登录身份鉴别、配置文件完整性保护、计算环境隔离与访问控制、密码设备运行状态监测、远程管理通道加密防护能力。

2.2.3 服务域

服务域面向可信数据空间服务平台、数字合约、数据目录、使用控制策略、运行维护系统，重点覆盖服务平台安全、合约安全、目录安全、策略安全、运维安全等场景。专用测评项包括以下内容。

设备和计算安全：核验服务器管理员登录身份鉴别、服务器固件完整性保护、计算环境隔离与访问控制、远程管理通道加密防护、服务器安全标识完整性保护能力。

应用和数据安全：核验数字合约全生命周期完整性保护（如基于 SM3 的区块链技术）、合约参与方电子签名、数据目录元数据脱敏与加密存储、使用控制策略签名与加密传输、服务运行日志存证脱敏与行为追溯能力。

2.2.4 计算域

计算域面向机密计算环境、密态计算节点、可信执行环境、可信平台模块等计算硬件，以及多方安全计算、密文计算业务，重点覆盖计算环境、计算过程、算法代码、计算数据 4 类安全维度。专用测评项包括以下内容。

设备和计算安全：核验计算硬件远程证明机制（如基于 SM2 数字签名）、计算环境隔离与访问控制、计算节点固件与代码完整性保护（如基于 SM3 哈希校验）、计算过程安全监控系统部署情况。

应用和数据安全：核验计算输入数据密态防护、计算中间结果加密存储、计算结果加密输出与授权访问、隐私计算与商用密码融合安全保障、计算行为不可否认与可追溯能力。

2.2.5　外部连通域

外部连通域面向跨可信数据空间互联、跨域安全网关、跨域数据摆渡、跨域身份与权限映射等业务对象，重点覆盖跨域互联安全、网关安全、摆渡安全、跨域数据安全、跨域权限安全等场景。专用测评项包括以下内容。

物理和环境安全：核验跨域网关机房密码门禁部署效果、互联节点物理非法接入防护措施、跨域环境审计日志加密与完整性保护能力。

网络和通信安全：核验跨域 TLCP 数据传输加密通道部署、跨域报文加密与签名配置、跨域安全网关双向身份鉴别、跨域数据安全流转机制、跨域通信实时监测能力。

设备和计算安全：核验跨域设备登录身份鉴别、固件完整性保护、设备计算环境隔离与访问控制、网关安全审计系统部署、远程管理通道加密防护能力。

应用和数据安全：核验跨域传输敏感数据加密保护、跨域数据标签完整性保护、跨域数据密级一致性保障、跨域操作行为签名存证、跨域数据使用权限动态管控能力。

3　可信数据空间商用密码应用指标体系与测评模型构建

3.1　指标体系框架

3.1.1　总体思路

结合可信数据空间安全域的架构特性、密码应用部署模式与典型风险场景，沿用 GB/T 39786—2021 与 GB/T 43206—2023 核心框架，搭建“一级指标（国标适配）—二级指标（安全域）—三级测评项（可信数据空间专项测评项）”的三层递进式技术指标体系，以及“一级指标（国标适配）—二级指标（可信数据空间管理维度测评项）”的两层管理指标体系。该体系既满足国标要求，又可与通用测评体系[18]衔接，能够作为现有密评体系的扩展补充。

3.1.2　指标对应关系

可信数据空间需满足 GB/T 39786—2021 规定的密码技术、密码产品与密码服务通用应用要求。在此基础上，从技术维度来看，可信数据空间安全域与 GB/T 39786—2021 安全层面对应关系如表 1 所示。

物理和环境安全层面：可信数据空间服务域、计算域仅涉及逻辑服务与计算环境，接入域、内部网络域及外部连通域需覆盖物理和环境安全相关要求。

网络和通信安全层面：接入域、外部连通域数据存在跨域传输需求，仅在本安全域内部节点之间进行服务域、计算域的数据传输。

设备和计算安全层面：5 大安全域均覆盖该层保护对象，具体对应为：接入域涉及接入节点设备；内部网络域涉及支撑空间通信链路的路由器、交换机等网络节点设备；计算域涉及承担安全防护、数据存储、内部计算与对外服务的服务器、密码存储及安全计算节点；外部连通域涉及跨域连通节点设备；服务域涉及数字合约、数据目录、存证清算等服务节点设备，包含服务器集群、虚拟化资源、边界安全设备、接入连接器服务端设备。

应用和数据安全层面：接入域涉及接入数据、接入身份、接入行为的密码安全管理；服务域涉及核心业务与数据全生命周期安全保护；计算域涉及密态计算过程及计算中间、结果数据保护；外部连通域涉及跨域数据流转与跨域应用行为保护；内部网络域无该层面专项保护需求。

表 1　可信数据空间安全域与 GB/T 39786—2021 安全层面对应关系

Table 1　Mapping between trusted data space security domains and GB/T 39786—2021 security layers

测评项	接入域	内部网络域	服务域	计算域	外部连通域
物理和环境安全	涉及	涉及	不涉及	不涉及	涉及
网络和通信安全	涉及	涉及	不涉及	不涉及	涉及
设备和计算安全	涉及	涉及	涉及	涉及	涉及
应用和数据安全	涉及	不涉及	涉及	涉及	涉及

3.2　测评模型构建

以 5 大安全域为切入点，结合通用网络与信息系统密评指标体系，从物理和环境安全、网络和通信安全、设备和计算安全、应用和数据安全 4 大技术维度，以及管理制度、人员管理、建设运行、应急处置 4 大管理维度搭建分层测评模型。依托安全域开展层级划分，可实现保护对象精细化归类，精准匹配各安全域对应的测评对象。

从技术维度和管理维度构建的可信数据空间密码应用指标体系及测评模型如表 2 和表 3 所示。

3.3　模型对比

由表 4 模型对比可知，通用信息系统密评框架（GB/T 43206—2023）面向传统单域信息系统，缺少对多主体、分布式、跨域数据空间的专项测评指标

（如合约签名、跨域权限映射、计算域远程证明）。国际数据空间框架（IDS/Gaia-X）侧重连接器组件一致性核验，未形成覆盖数据空间全域的测评指标体系。本文模型通过安全域解耦与国标层面双向映射，系统性地将外部连通域纳入密评范围，并针对密态计算、数字合约、跨域协同等数据空间特有场景设计了专项测评项，在测评覆盖范围、场景适配能力和国标衔接效果上具有明显优势。

表 2 可信数据空间密码应用指标体系及测评模型（技术维度）

Table 2 Trusted data space cryptographic application indicator system and evaluation model (technical dimensions)

技术要求	安全域	测评项
物理和环境安全	接入域/内部网络域/外部连通域	1）密码设备、接入设备、网络设备、计算设备、存储设备以及服务设施等所在的机房，部署采用密码技术（如基于SM2的数字签名验证、基于SM4的CBC-MAC机制等）的电子门禁，确保进入人员身份的真实性； 2）采用密码技术保证机房电子门禁进出记录数据的存储完整性； 3）采用密码技术保证机房视频监控影像记录的完整性
网络和通信安全	接入域	1）在接入边界部署接入节点（如安全认证网关），实现对接入终端的身份鉴别与访问控制； 2）接入节点采用密码技术，确保内部存储的访问控制信息的完整性； 3）接入链路采用基于密码的安全通信协议（如TLCP）构建安全通道，确保通信过程中数据的完整性和机密性； 4）如果接入节点设备是通过公共网络，则采用专用安全线路（如IPSec）与可信数据空间内部节点连接，并采用密码技术对接入节点设备身份核验； 5）对3）中的安全通道状态进行定期检测，确保通信安全； 6）采用密码技术结合特征检测，实现边界隐写数据过滤与恶意数据拦截
	内部网络域	1）内部节点之间通信采用密码技术进行身份鉴别，确保节点身份真实性； 2）内部节点之间采用基于密码的安全通信协议，确保通信过程中数据的完整性和机密性； 3）部署密码安全监测系统，实时监控内部节点之间的通道安全状态
	外部连通域	1）跨可信数据空间的网络通信，采用密码技术对通信节点进行身份鉴别，确保身份真实性； 2）跨可信数据空间的网络通信，采用基于密码的安全通信协议，确保通信过程中数据的完整性和机密性
设备和计算安全	接入域	1）管理员登录设备时，采用密码技术进行身份鉴别，确保身份真实性； 2）当管理员用户远程登录接入节点设备时，采用密码技术建立安全传输通道。 3）采用密码技术保障接入节点设备资源访问控制信息的完整性； 4）采用密码技术保障接入节点设备重要信息资源安全标记的完整性； 5）采用密码技术保障接入节点设备操作日志和运行日志的完整性； 6）采用密码技术保障接入节点设备内软件/固件的完整性和真实性（如SM2代码签名）
	内部网络域	1）管理员登录路由器、交换机等网络节点设备时，采用密码技术进行身份鉴别，确保身份真实性； 2）当管理员远程登录网络节点设备时，采用密码技术建立安全传输通道； 3）采用密码技术保证网络节点设备资源访问控制信息的完整性； 4）采用密码技术保证网络节点设备重要信息资源安全标记的完整性； 5）采用密码技术保证网络节点设备操作日志和运行日志的完整性； 6）采用密码技术保证网络节点设备内软件/固件的完整性和真实性（如SM2代码签名）
	计算域	1）管理员登录设备时，采用密码技术进行身份鉴别，确保身份真实性； 2）当管理员远程登录计算节点设备时，采用密码技术建立安全传输通道； 3）采用密码技术保障计算节点设备资源访问控制信息的完整性； 4）采用密码技术保障计算节点设备重要信息资源安全标记的完整性； 5）采用密码技术保障计算节点设备操作日志和运行日志的完整性； 6）采用密码技术保障计算节点设备内重要可执行程序的完整性和真实性（如SM2代码签名）； 7）承载对外服务功能的计算环境采用物理、虚拟或容器隔离技术，结合密码技术实现访问控制； 8）承载敏感计算（如密钥存储、密码运算、随机数生成）的机密计算环境支持基于密码技术的远程证明，确保环境固件和硬件的可信性； 9）采用密码技术保障计算资源调度信息的完整性； 10）部署计算过程安全监控系统，实时监测计算行为

续表 2

技术要求	安全域	测评项
设备和计算安全	服务域	1）采用密码技术对登录服务器的用户进行身份鉴别，确保用户身份真实性； 2）采用密码技术保证服务器固件的完整性，采用SM3 哈希校验； 3）服务计算环境采用物理或虚拟隔离技术，结合密码技术实现访问控制； 4）远程管理服务器时采用密码技术建立安全传输通道； 5）采用密码技术保证服务器安全标记的完整性
	外部连通域	1）管理员登录跨域连通设备时，采用密码技术进行身份鉴别，确保身份真实性； 2）当管理员用户远程登录连通节点设备时，采用密码技术建立安全传输通道； 3）采用密码技术保证连通节点设备资源访问控制信息的完整性； 4）采用密码技术保证连通节点设备重要信息资源安全标记的完整性； 5）采用密码技术保证连通节点设备操作日志和运行日志的完整性； 6）采用密码技术保证连通节点设备内软件/固件的完整性和真实性
应用和数据安全	接入域	1）接入主体身份采用商用密码数字凭证进行鉴别，并支持 SM2 算法的身份校验； 2）采用基于商用密码密钥的多因素核验机制，提升接入身份认证强度； 3）接入数据采用商用密码算法加密上传，解密过程需授权管控； 4）采用商用密码算法保证接入数据标签的完整性，避免标签篡改； 5）采用密码技术保证接入数据使用行为的可追溯
	服务域	1）数字合约全生命周期采用密码技术，确保加解密过程完整性和可追溯性； 2）采用密码技术，保证数字合约参与方行为的不可否认性； 3）采用密码技术对数据目录元数据进行脱敏和加密存储； 4）采用密码技术保证控制策略传输和存储的完整性与机密性； 5）采用密码技术保证管理日志、运行日志的完整性； 6）采用密码技术保证数据目录查询行为的隐私性； 7）使用密码技术，确保数据使用控制实现双重授权； 8）使用密码技术，确保授权信息安全转换为策略引擎的执行规则（策略引擎的执行规则来源于数据所有者和平台可信服务商）
	计算域	1）计算输入数据采用 SM4 算法加密保护，进入密态计算过程； 2）计算中间结果采用 SM4 算法加密存储，防止数据泄露； 3）计算结果应采用 SM4 算法加密输出，仅授权主体可解密访问； 4）隐私计算技术应与商用密码算法融合，无安全漏洞； 5）采用密码技术保证计算行为的不可否认性与可追溯性
	外部连通域	1）跨域传输的敏感数据采用商用密码算法加密保护； 2）采用商用密码算法保证跨域数据标签的完整性，防止标签篡改； 3）采用密码技术保证跨域数据密级一致性，避免密级降级； 4）跨域操作行为采用密码技术进行签名存证，保证行为可追溯； 5）采用密码技术实现跨域数据使用权限的动态管控

表 3　可信数据空间密码应用指标体系与测评模型（管理维度）

Table 3　Trusted data space cryptographic application indicator system and evaluation model (management dimensions)

管理维度	测评项
管理制度	1）制定覆盖可信数据空间全场景的商用密码应用管理制度，明确接入域、内部网络域、服务域、计算域、外部连通域的密码应用职责与操作流程； 2）制定跨域密码协同管理规范，明确不同数据空间之间密码策略、证书、密钥的统一管理要求； 3）建立数字合约密码应用管理规范，明确签名、存证、加密、核验要求； 4）制定密态计算、隐私计算密码使用规范，确保算法合规、密钥安全； 5）建立数据目录与使用控制策略的密码保护管理规范； 6）要求跨域互通网关、连接器统一执行密码策略与准入规则

续表 3

管理维度	测评项
人员管理	1）明确各安全域密码管理岗位设置与职责分工，配备专职密码管理员； 2）建立密码岗位责任制，明确密码管理员、安全管理员、审计管理员三员分立
建设运行	1）可信数据空间在规划、设计、建设、验收、运行、升级的全生命周期中，应同步开展密码应用的设计与实施； 2）接入连接器、服务平台、计算节点上线前应完成密码应用方案评审与检测； 3）建立密码设备（密码机、HSM、签名验签服务器、商用密码网关）台账管理与运行监测机制； 4）对密码配置、策略、证书、密钥变更执行审批、记录、审计流程，禁止未授权修改； 5）定期开展密码应用合规性自查，覆盖五大安全域密码功能有效性； 6）第三方接入、跨域接入、新节点接入时，应进行密码应用安全性审查； 7）建立覆盖全空间、全节点、全业务的密钥全生命周期管理制度； 8）跨域密钥、计算密钥、合约密钥、接入密钥、通信密钥应分类分级管理； 9）核心密钥必须在HSM中存储、使用，严禁以明文形式导出； 10）数字证书应由合法CA颁发，建立证书申请、颁发、更新、吊销、归档机制； 11）定期开展密钥与证书有效性检查、过期预警、强制更新； 12）建立密码操作审计策略，覆盖身份认证、加解密、签名验签、密钥操作、证书操作等行为； 13）审计记录应采用密码技术防篡改、防删除、防伪造，保存时间满足法律法规要求； 14）支持跨域审计日志汇聚与关联分析，实现全域密码行为可追溯
应急处置	1）制定密钥泄露、证书伪造、加密通道破解、跨域安全事件等密码专项应急预案； 2）建立跨主体、跨安全域、跨数据空间的应急协同处置机制 3）发生密码安全事件时，能够快速隔离、紧急更换密钥 / 证书、阻断攻击、留存证据； 4）应急处置过程应全程记录、审计、复盘，并完善密码防护策略； 5）每年至少开展 1 次密码安全应急演练

表 4　模型对比

Table 4　Model comparison

对比维度	通用信息系统密评框架 (GB/T 43206—2023)	国际数据空间框架 (IDS/Gaia-X)	本文模型
安全域划分	无显式安全域划分， 按资产类型组织	偏重连接器与通信组件	明确划分接入/内部网络/服务/计算/ 外部连通五大安全域
与GB/T 39 786 安全层面映射关系	直接映射（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）	不适用（非国标体系）	5大安全域与4个技术层面双向映射， 管理维度全覆盖
跨域适配	弱（未覆盖跨主体）	中（侧重策略互认）	强（DID互认+联邦KMS+策略同步）
跨域密钥协同管理测评	否	部分	是（管理维度含跨域密钥分级、证书统一管理）
数字合约、使用控制策略专项测评	否	部分（使用控制）	是（服务域合约/目录/策略全流程）
机密计算远程证明测评	否	否	是（计算域远程证明测评项）
数据行为追溯	采用事后审计的方法进行数据行为追溯，易被篡改	建议采用存证架构进行数据行为追溯	新增数据流通全链路行为可溯专项指标：跨域操作日志的国密SM3哈希锚定率；区块链存证数据与原始日志的一致性比对通过率；溯源查询响应时间与完整性证明生成能力

4　指标体系与测评模型理论分析

考虑到目前国家级可信数据空间技术路线仍在建设过程中，尚不具备测试验证环境，因此，本文采用理论分析法，将安全风险、安全保障措施与测评指标逐项匹配，验证测评模型与指标的完备性、落地可行性。同时对标 GB/T 39786—2021、GB/T 43206—2023，核验密码应用测评覆盖全面性，确保本文建

立的测评体系能够覆盖测评通用要求。

4.1　技术维度理论分析

本节针对可信数据空间各安全域的典型安全风险，逐一分析对应的密码测评要点，理论分析结果分别如表 5~表 9 所示。其中“●”代表能够有效应对，“—”代表暂无有效措施应对。

4.1.1　接入域理论分析

针对接入域接入身份被冒用、伪造风险，在网络和通信安全层面，可核验系统是否采用 SM2 数字签名完成身份鉴别、部署商用密码网关完成边界认证；在设备和计算安全层面，可核验接入设备身份鉴别、固件完整性防护机制；在应用和数据安全层面，可核验数字凭证鉴别、多因素认证落地情况。

针对绕过身份核验、非法接入风险，在网络和通信安全层面，可核验边界身份认证、接入链路加密及节点双向身份鉴别机制部署情况；在设备和计算安全层面，可核验计算环境隔离、细粒度访问控制、远程管理通道加密能力。

表 5　接入域测评项理论分析结果

Table 5　Theoretical analysis of access domain evaluation items

测评项	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
接入身份被冒用、伪造	—	●	●	●
绕过身份核验、非法接入	—	●	●	—

表 6　内部网络域测评项理论分析结果

Table 6　Theoretical analysis of internal network domain evaluation items

测评项	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
网络通信被窃听、数据被篡改	—	●	—	—
会话密钥协商被破解、通信内容泄露	—	●	—	—

4.1.2　内部网络域理论分析

针对网络通信被窃听、数据被篡改等风险，在网络和通信安全方面，可核验 SM4 传输加密、SM3 完整性校验、加密传输通道部署情况。

针对会话密钥协商被破解、通信内容泄露等风险，在网络和通信安全测评方面，可采用 SM2 双向认证、安全密钥协商机制。

表 7　服务域测评项理论分析结果

Table 7　Theoretical analysis of service domain evaluation items

测评项	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
数字合约被篡改	—	—	—	●
数据目录查询请求被劫持	—	—	—	●
使用控制策略传输 / 存储泄露或篡改	—	—	—	●
日志存证泄露、可篡改	—	—	●	●

表 8　计算域测评项理论分析结果

Table 8　Theoretical analysis of computing domain evaluation items

测评项	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
计算环境安全风险	—	—	●	—
计算过程数据安全风险	—	—	●	●

表 9　外部连通域测评项理论分析结果

Table 9　Theoretical analysis of external connectivity domain evaluation items

测评项	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
跨域身份权限映射风险	●	●	●	●
跨域数据安全传输风险	—	●	—	●

4.1.3　服务域理论分析

针对数字合约被篡改风险，在应用和数据安全层面，核验合约 SM3 完整性校验、区块链存证、SM2 签名校验机制。其余安全维度不具备合约防篡改防护能力。

针对数据目录查询请求被劫持风险，在应用和数据安全层面，核验目录加密、细粒度访问控制机制。其余安全维度无法抵御该类劫持风险。

针对使用控制策略传输、存储泄露或篡改风险，在应用和数据安全层面，核验策略加密传输、加密存储与签名校验机制。

针对日志存证泄露、篡改风险，在设备和计算安全层面，核验服务器操作日志完整性保护机制；

在应用和数据安全层面，核验日志加密存证、内容脱敏与完整性防篡改机制。

4.1.4 计算域理论分析

针对计算域的计算环境安全风险，在设备和计算安全层面，依托计算硬件 SM2 远程证明、计算环境隔离与访问控制、固件/代码 SM3 完整性保护，从设备层保障计算环境不被突破、非法篡改；应用和数据安全层面无直接防护手段，无法保障计算环境本体安全。

针对计算过程数据安全风险，在设备和计算安全层面，依托计算过程安全监控、计算环境隔离，防范计算过程中数据被非法窃取、篡改；在应用和数据安全层面，依托计算输入、中间结果全流程 SM4 加密、隐私计算与商用密码融合、计算结果 SM2 签名存证，从数据层保障计算全流程数据安全。

4.1.5 外部连通域理论分析

针对跨域身份权限映射风险，在物理和环境安全层面核验跨域网关机房密码门禁、物理访问控制、操作日志加密存证，防范未授权人员篡改身份/权限配置；在网络和通信安全层面，通过跨域安全网关 SM2 身份校验、跨域双向身份认证，从通信层验证身份真实性，防范身份冒用/权限溢出；在设备和计算安全层面，依托跨域设备身份鉴别、计算环境隔离与密码访问控制，从设备层限制非法身份接入、越权操作；在应用和数据安全层面，依托跨域操作 SM2 签名存证、跨域权限动态管控、数据密级一致性保障，从应用层绑定身份与权限，规避映射逻辑混乱。

针对跨域数据安全传输风险，在网络和通信安全层面，搭建跨域 TLCP 加密通道，采用报文 SM4 加密与 SM3 完整性签名，从通信层保障传输机密性、完整性，抵御窃听、篡改攻击；在应用和数据安全层面，对跨域敏感数据进行 SM4 加密、数据标签 SM3 完整性校验，从数据层保障传输数据安全，防范数据泄露、标签篡改。

4.2 管理维度理论分析

本文提出的可信数据空间管理维度密码应用测评指标体系，从管理制度、人员管理、建设运行、应急处置等方面均覆盖 GB/T 39786-2021 管理要求。在此基础上，本文面向可信数据空间分布式跨域、多主体、密态计算、数据可用不可见等特有架构，对管理维度进行场景化、体系化、全域化创新扩展。

4.3 与传统测评体系的差异分析

对比传统网络信息系统，本文提出的可信数据空间的密码应用指标与测评模型具有以下差异。

1）系统架构不同，安全域映射关系存在区别。可信数据空间采用“分布式联邦架构”，突破了传统网络与信息系统“单中心集中式”架构下单一主体、单一安全边界的限制。搭建测评模型时需覆盖接入域、内部网络域、服务域、计算域、外部连通域 5 大安全域，重点关注跨域身份互信、跨空间策略一致性、分布式密钥协同管控等传统测评模型尚未覆盖的测评要点。

2）安全防护目标不同，新增专属测评指标。传统网络与信息系统的密码应用与测评更加关注“系统安全”“边界防护”，而可信数据空间诞生初衷是保障数据可管可控流通。本文所提出的测评模型紧扣“数据不出域、可用不可见、可控可计量”的安全目标，在传统密评聚焦系统身份认证、传输及存储安全的基础上，拓展数字合约签名、数据目录保护、数据使用权限管控、密态计算、跨域数据摆渡等可信数据空间专属测评项。

3）测评场景不同，兼顾新技术融合运用。可信数据空间引入密态计算、多方安全计算等新技术，因此，在指标设计上新增密态计算正确性、密码算法一致性、计算结果完整性与可验证性等测评内容，适配可信数据空间特有的业务模式与安全需求。

4.4 测评模型场景化应用分析

以某市“城市可信数据空间”为应用场景，基于其“三统一”数据基础设施（统一接口管理、统一身份登记、统一目录标识），结合平台技术架构（如图 4 所示）推演测评模型的落地应用过程。其核心安全诉求为原始数据不出域，仅输出计算结果；所有流通数据全流程密态保护；数据流通行为全链路可追溯、可审计；满足安全监管要求。

结合该市可信数据空间创新试点背景，选取该城市可信数据空间“三统一”数据基础设施作为测评模型场景化应用分析对象。本示例聚焦单个可信数据空间内部，不涉及跨数据空间互联互通场景，因此，外部连通域暂不纳入本次测评范围。测评模型应用分析如表 10 所示，关键测评项选取示例如表 11 所示，测评方法及预期结果示例如表 12 所示。

5 结束语

本文面向可信数据空间分布式架构特征，以及“集中管控、分布执行、数据不出域、可用不可见”的核心功能，针对现有通用商用密码应用标准及测

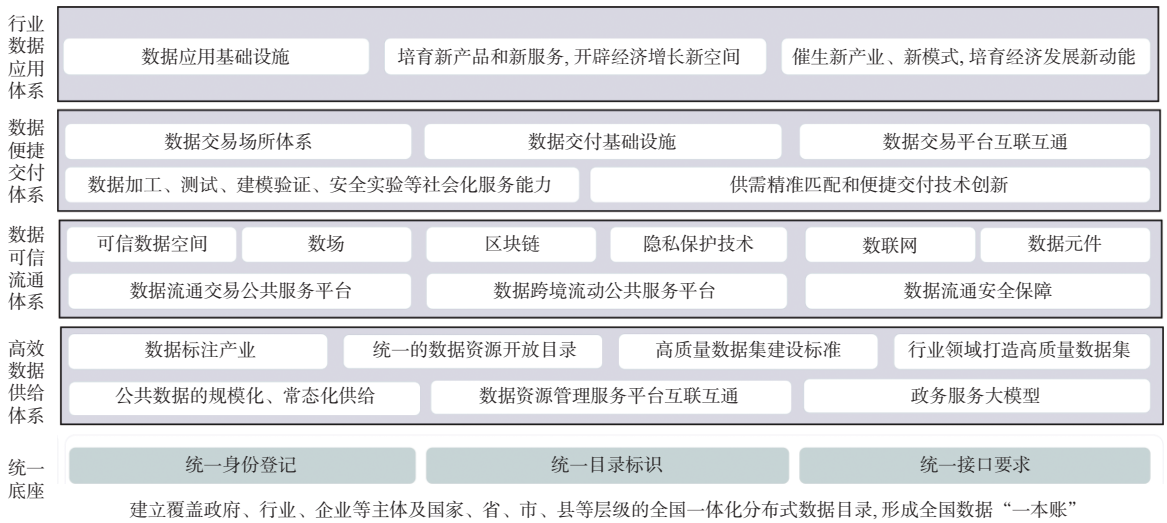

图 4　“三统一”架构

Fig. 4　"Three unifications" architecture

表 10　测评模型应用分析

Table 10　Evaluation model application analysis

“三统一”要素	功能定位	对应论文安全域
统一身份登记	统一登记和认证体系，便于不同基础设施身份互信互认	接入域
统一目录标识	使用相同的标识体系，便于实现标识之间相互解析	服务域/计算域
统一接口管理	实现各系统之间身份、目录、标识等上报、同步、查询、下发接口标准化	接入域/内部网络域

表 11　关键测评项选取示例

Table 11　Selection examples of key evaluation items

安全域	统一要素	测评对象	测评内容
接入域	统一身份登记	统一身份认证系统	接入终端是否采用SM2数字证书进行双向身份鉴别，参与方用户是否采用SM2证书+动态口令多因素认证
		跨域身份映射模块	跨域身份映射是否采用SM2签名验证+权限最小化
接入域/内部网络域	统一接口管理	API网关	接入接口是否采用TLCP加密通道+SM2双向鉴别
内部网络域	统一接口管理	通信协议栈	节点间通信是否采用国密算法（SM2/SM3/SM4）
内部网络域	统一接口管理	数据格式转换模块	接口数据格式转换过程是否持续密码保护
服务域	统一目录标识	统一数据目录系统	数据目录元数据是否采用SM4加密+细粒度访问控制
		数据目录查询接口	数据目录查询行为是否采用密码技术保护隐私
		数据标识管理模块	数据标识是否采用SM3杂凑保证唯一性和完整性
		数字合约管理模块	数据使用合约是否采用SM3+区块链存证、多方SM2签名
		使用控制策略引擎	使用控制策略传输存储是否经SM4加密+SM3完整性保护
计算域	统一目录标识	数据库TEE	机密计算节点是否支持基于SM2的远程证明
		密态计算引擎	计算输入/中间/输出是否全流程SM4加密
		计算结果存证模块	计算结果是否采用SM2签名保证完整性和可追溯性

续表 11

安全域	统一要素	测评对象	测评内容
管理维度	“三统一”支撑	密钥管理系统	密钥是否分类分级管理，核心密钥是否存储在HSM中
		证书管理系统	证书是否由合法CA颁发，建立证书全生命周期管理
		审计日志系统	审计日志是否采用密码技术防篡改，支持跨域汇聚
		应急响应机制	是否建立跨主体的应急协同处置机制

表 12 测评方法及预期成果选取示例

Table 12 Examples of selected evaluation items and expected outcomes

测评项	测评方法	预期结果
统一身份登记–接入鉴别	抓取身份认证系统的握手报文，检查证书链	使用CA签发的SM2证书，双向验证
统一身份登记–多因素认证	尝试使用错误/过期动态口令登录连接器管理系统	拒绝登录，记录审计日志
统一身份登记–跨域映射	使用不同域的身份凭证尝试跨域访问	映射正确，权限最小化
统一目录标识–目录加密	检查数据目录数据库存储状态	元数据为SM4密文，无权限用户无法解析
统一目录标识–查询隐私	抓取数据目录查询请求报文	查询内容加密，无法识别具体查询条件
统一目录标识–标识完整性	篡改数据标识后验证完整性校验	完整性校验失败，系统告警
统一目录标识–合约存证	查询数据使用合约的区块链存证记录	合约存证哈希存在，各方SM2签名有效
统一目录标识–策略保护	篡改策略内容后发送给策略引擎	签名校验失败，引擎拒绝执行
统一目录标识–远程证明	调用TEE证明接口，验证SM2签名，比对PCR值	远程证明有效，PCR值与基线一致
统一目录标识–全流程密态	在数据库入口和出口抓包，检查中间存储	输入/中间/输出均为SM4密文
统一目录标识–结果存证	获取计算结果并验证SM2签名	签名有效，可追溯计算主体和时间
管理–密钥管理	检查KMS配置和HSM部署情况	密钥分类分级，核心密钥在HSM中
管理–证书管理	审查证书管理文档，检查过期预警配置	建立证书全生命周期管理机制
管理–审计追溯	从审计平台查询一笔数据交易的完整调用链	审计日志可关联追溯，SM2签名完整
管理–应急协同	查看应急预案和演练记录	明确跨主体应急流程，每年至少演练1次

评框架难以覆盖其特殊性的问题，开展可信数据空间商用密码应用指标体系与测评模型构建研究。

首先，基于可信数据空间核心架构，将逻辑层级解耦为接入域、内部网络域、服务域、计算域、外部连通域 5 大安全域，系统梳理各安全域典型密码安全风险，形成全场景密码应用防护思路与测评需求，明确了面向可信数据空间的密评对象与覆盖范围。

其次，在沿用 GB/T 39786—2021 与 GB/T 43206—2023 通用要求及基本框架基础上，搭建包含技术维度（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）、管理维度（制度/人员/运行/应急）的测评模型，补充可信数据空间全场景、数据全生命周期专属测评内容，突破传统信息系统“单平台、单边界”密码应用及评估模式，将密码应用及测评思路延伸至 5 大安全域全链路，实现从接入、网络、服务、计算到跨域互通的全域密码策略统一、职责统一、流程统一，解决分布式架构下密码应用及测评碎片化问题。

本文相关研究成果能够推动可信数据空间密码应用及安全性评估架构、指标、模型三重创新，具备较强科学性与可操作性，可为可信数据空间密码应用方案设计、建设实施、安全测评与整改优化提供统一框架与实施依据，对支撑数据要素安全合规流通、推动商用密码在数据基础设施中深度落地具有重要理论价值与现实意义。

参考文献：

[1] 国家数据局. 可信数据空间发展行动计划（2024—2028 年）：国数资源〔2024〕119 号 [EB/OL]. （2024-11-21） [2025-12-12]. https://www.gov.cn/zhengce/zhengceku/202411/content_6996363.htm.
National Data Administration. Action plan for the development of trusted data spaces （2024—2028）：No. 119 of national data resources〔2024〕[EB/OL]. （2024-11-21） [2025-12-12]. https://www.gov.cn/zhengce/zhengceku/202411/content_6996363.htm.

[2] 董贵山, 白健, 王浚侨. 基于密码的数据安全体系研究 [J]. 信息安全与通信保密，2025（4）：62-74.
Dong G S, Bai J, Wang J Q. Research on cryptography-based data security architecture[J]. Information Security and Communications Privacy，2025（4）：62-74.

[3] 赵一鸣，黄丹迪. 我国可信数据空间的建设原则与发展路径 [J]. 现代情报，2025，45（6）：126-139.
Zhao Y M，Huang D D. Construction principles and development paths of trusted data spaces in China[J]. Journal of Modern Information，2025，45（6）：126-139.

[4] International Data Spaces Association. IDS reference architecture model V4.0[S]. 2023.

[5] Khan S，Madnick S. Cybersafety：a system-theoretic approach to identify cyber-vulnerabilities and mitigation requirements in industrial control systems[J]. IEEE Transactions on Dependable and Secure Computing，2022，19（5）：3312-3328.

[6] 全国信息安全标准化技术委员会. 信息安全技术 信息系统密码应用基本要求：GB/T 39786-2021 [S]. 北京：中国标准出版社，2021.
National Information Security Standardization Technical Committee. Information security technology—basic requirements for cryptographic application in information systems：GB/T 39786-2021[S]. Beijing：China Standards Press，2021.

[7] Gaia-X European association for data and cloud. gaia-x framework document v2.2[EB/OL]. （2023-10-15） [2025-12-12]. https://gaia-x.eu.

[8] NIST. IR 8451：Zero trust architecture for data spaces[R]. Gaithersburg：NIST，2023.

[9] ISO/IEC 27040：2023. Information technology—security techniques—storage security[S]. Geneva：ISO，2023.

[10] 李高磊，李建华，周志洪. 面向新型关键基础设施的密码应用安全性评估技术综述 [J]. 网络与信息安全学报，2023，9（6）：1-19.
Li G L，Li J H，Zhou Z H. Overview of security assessment technologies for cryptographic applications in new critical infrastructures[J]. Chinese Journal of Network and Information Security，2023，9（6）：1-19.

[11] 全国数据标准化技术委员会. 可信数据空间技术架构 [Z]. 2025-04.
National Data Standardization Technical Committee. Technical architecture of trusted data space[Z]. 2025-04.

[12] ETSI TS 133501 V15.1. 0 （2018-07）. Security architecture and procedures for 5G system （3GPP TS 33.501 version 15.1. 0 Release 15）[S].

[13] 全国网络安全标准化委员会. 可信数据空间密码保障体系研究 [Z]. 2025-10.
National Cybersecurity Standardization Technical Committee. Research on cryptographic assurance system for trusted data space[Z]. 2025-10.

[14] 冯登国. 机密计算发展现状与趋势 [J]. 信息安全研究，2024，10（1）：1-8.
Feng D G. Current status and trends of confidential computing[J]. Journal of Information Security Research，2024，10（1）：1-8.

[15] Gieß A，et al. What does it take to connect unveiling characteristics of data space connectors[C]//Proceedings of the 57th Hawaii International Conference on System Sciences （HICSS）. Honolulu，Hawaii，USA，2024.

[16] 全国信息安全标准化技术委员会. 信息安全技术 信息系统密码应用测评要求：GB/T 43206-2023 [S]. 北京：中国标准出版社，2023.
National Information Security Standardization Technical Committee. Information security technology—evaluation requirements for cryptographic application in information systems：GB/T 43206-2023[S]. Beijing：China Standards Press，2023.

[17] 冯登国，林璟锵，荆继武，等. 数据要素流通中的密码技术体系架构 [J]. 密码学报，2024，11（2）：245-260.
Feng D G，Lin J Q，Jing J W，et al. Architecture of cryptographic technology system in data element circulation[J]. Journal of Cryptologic Research，2024，11（2）：245-260.

[18] 中国密码学会. 商用密码应用安全性评估指南 （第二版）[M]. 北京：电子工业出版社，2022.
China Cryptography Society. Guide to security assessment of commercial cryptography application （2nd edition）[M]. Beijing：Publishing House of Electronics Industry，2022.