TC609

全国数据标准化技术委员会技术文件

TC609-6-2025-XX

可信数据空间 使用控制技术要求

Trustworthy data space—Technical requirements for usage control

（征求意见稿）

2025-XX-XX 发布　　2025-XX-XX 实施

全国数据标准化技术委员会　发布

目　　次

前　　言

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。
本文件由全国数据标准化技术委员会（SAC/TC609）提出并归口。
本文件起草单位：

可信数据空间 使用控制技术要求

1 范围

本文件规范了可信数据空间中使用控制的技术要求，包括功能要求、接口规范和安全要求。

本文件适用于可信数据空间中数据使用控制功能的设计和开发，可为可信数据空间服务平台和接入连接器的数据使用控制模块的建设、运行和评估提供参考。

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。

NDI—TR—2025—02 数据基础设施 互联互通基本要求

NDI—TR—2025—04 数据基础设施 标识管理规范

TC609—6—2025—01 可信数据空间 技术架构

3 术语和定义

下列术语和定义适用于本文件。

3.1

可信数据空间 trustworthy data space

基于共识规则，联接多方主体，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。

[来源：TC609—6—2025—01 可信数据空间 技术架构]

3.2

使用控制 usage control

在数据的传输、存储、使用和销毁环节，通过集成在数据应用、算法和运行环境中的技术手段，确保相关参与方按照数字合约约定的使用策略对数据进行分析、计算和处理等，实现对数据使用的时间、地点、主体、行为和客体等因素的控制，从而保证对数据的使用符合预期。

[来源：TC609—6—2025—01 可信数据空间 技术架构]

3.3

数字合约 digital contract

以数字化形式描述的数据提供方、数据使用方、数据服务方等相关参与方对数据流通、使用等环节预期的承诺，包括但不限于数据的内容、使用者、使用方式、使用次数、使用范围、使用环境等。

[来源：TC609—6—2025—01 可信数据空间 技术架构]

3.4

数据沙箱 data sandbox

是一种可信数据管控技术，通过构建一个应用层隔离环境，允许数据提供方、使用方、服务方在安全隔离的区域内对数据进行使用、分析、处理、计算和结果输出。

3.5

使用控制策略引擎 usage control policy engine

可信数据空间中负责解析、评估与执行使用控制策略的能力组件，以数字合约内策略要求为依据，对数据使用行为进行细粒度、动态、可追踪的控制。

3.6

行为校验 behavior verification

基于预设策略和当前上下文信息，对数据使用请求进行可执行校验并生成允许或拒绝等控制结果的过程。

3.7

操作执行 operation execution

基于行为校验结果，对数据分析、计算、处理和下载等使用行为进行控制执行的过程。

4 概述

使用控制技术是可信数据空间“符合预期”的关键，通过使用控制技术可实现数据访问、分析、计算和销毁等行为的管控，从而保证双方对数据的使用符合预期，并结合数据沙箱、隐私保护计算等技术共同实现数据流通利用过程的“可信”。

接入连接器作为数据实际使用的执行点，是策略执行节点和数据使用环境的载体，功能包括策略解析、行为校验、环境构建、操作执行和行为记录与存证回传等，需动态应对使用过程中的环境变化和使用异常等情况。当连接器功能不足以满足数字合约预定的操作或约束条件时，或者两个异构接入连接器进行数据交互时，可信数据空间服务平台可为多接入连接器提供集中式的使用控制环境，确保数据访问、分析、计算和销毁等行为的管控。另外，可信数据空间服务平台作为策略管理方，功能侧重于策略的标准化生成、合约绑定、统一下发和履约管理，确保策略规则合规和控制执行路径可实现，目的是通过建立统一的交互流程、策略模板和接口规范将使用方行为约束落地到不同接入连接器、使用环境、算法模型和应用程序中。

本标准围绕“环境安全、执行可信、行为可证”目标展开，将明确可信数据空间服务平台与接入连接器间的数据使用控制交互流程，明确功能要求、接口规范和安全要求。

5 总体架构

5.1 功能架构

5.1.1 接入连接器使用控制功能框架

接入连接器需具备可信的控制策略执行、数据使用环境和使用存证功能。控制策略执行具有策略解析、行为校验、操作执行等功能；数据使用环境包括软硬件环境、算法应用、使用监控功能；使用存证方面支持细粒度的日志记录，支持查询和审计追溯，并按照要求上报给可信数据空间服务平台，便于统一的数据使用控制管理和追溯。

接入连接器的使用控制功能旨在确保可信数据空间中数据在交付与使用全过程可控、可审计。框架设计遵循“平台集中治理—连接器本地执行”的原则，将服务平台的全局策略管理与多连接器适配能力，转化为连接器端的精确执行与反馈机制。在**数据使用环境**方面，连接器侧重于提供与策略声明匹配的发送、接收及必要处理能力，不追求全功能计算环境，而是面向数据提供方和使用方的实际部署条件，实现最小化、隔离化的安全环境，确保跨组织传输与本地处理环节均符合策略要求。在**控制策略执行**方面，连接器承担策略解析后的本地化执行职能，重点落实数据交付策略（包括前置处理、交

付方式、协议选择等）、使用过程策略（访问、复制、存档、分发、使用等行为限制）以及通用约束策略（如访问白名单、规则匹配等），并通过技术手段保证策略不可绕过、不可篡改。在**使用存证**方面，连接器不仅记录操作日志，还应按策略声明的粒度实时生成可验证的存证信息，并安全上报服务平台，实现平台端的全局审计与本地端的行为固化。整体框架通过这种分层分工，既保证了策略的灵活适配，又在连接器侧形成可独立运行的可信执行闭环。

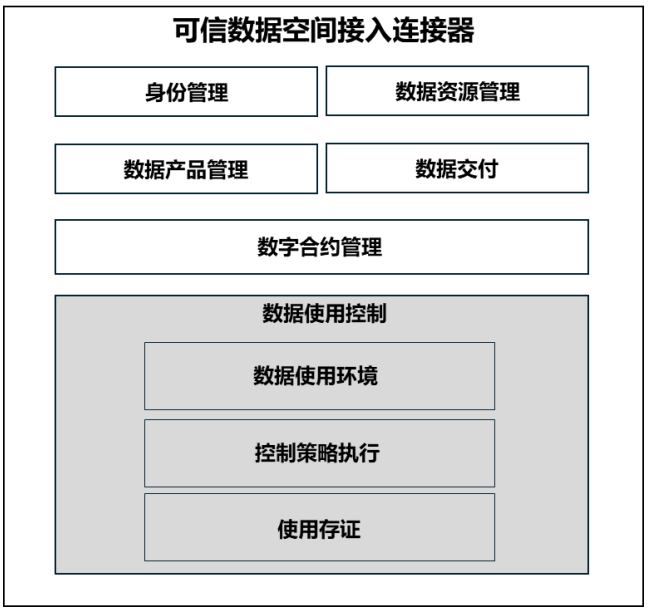

图1 接入连接器数据使用控制功能框架图

5.1.2 可信数据空间服务平台使用控制功能框架

可信数据空间服务平台使用控制功能包含数据使用环境、控制策略执行和使用存证功能。平台在数据使用环境方面，提供隔离、安全、可度量的运行与存储环境，并支持多类型环境的统一管理与调度；提供集中式使用控制能力，涵盖策略管理、策略支持、策略解析、行为校验与操作执行等细分功能，为接入连接器提供多样的使用控制策略和算法应用服务，支持异构接入连接器的动态适配，对数据访问、处理、分发等行为进行实时校验与控制，并保障执行结果符合策略约定；在使用存证方面，具备对数据交付、使用过程的全链路记录与追溯能力。

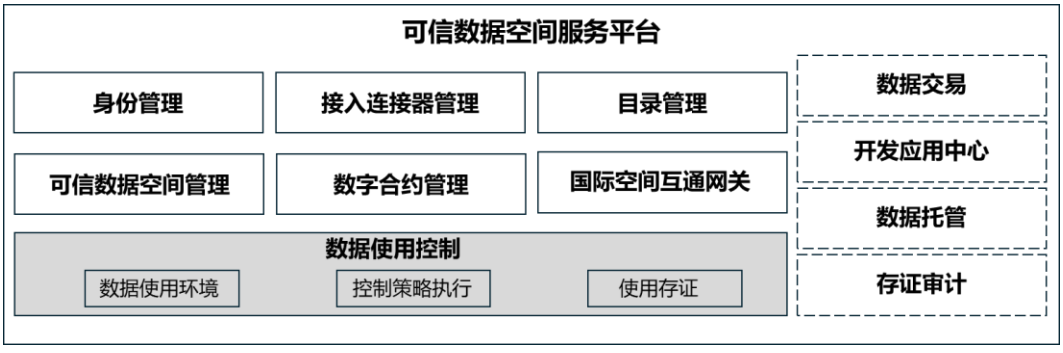

图2 可信数据空间服务平台数据使用控制功能框架图

5.2 交互过程

5.2.1 数据提供方接入连接器和使用方接入连接器交互

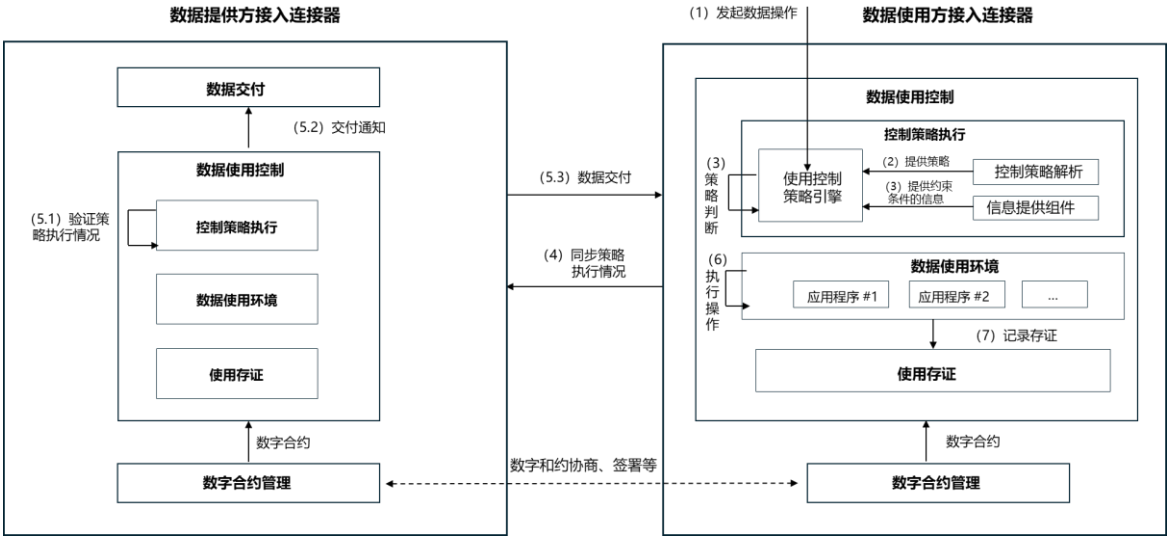

图3 数据提供方接入连接器和数据使用方接入连接器的使用控制交互流程图

数据提供方和数据使用方可通过可信数据空间服务平台完成数字合约的协商和签署，并由服务平台下发数字合约至双方接入连接器，也可双方直接协商形成数字合约。使用控制模块中的控制策略解析模块从数字合约中解析出数据产品对应的使用控制策略（包含操作行为和约束条件等）并安全保存，交互过程如下：

1. 发起数据使用操作：数据使用方在己方接入连接器上发起数据使用操作，操作信息包含数据产品、使用方式、使用者信息等；
2. 获取数据使用策略：在数据使用方接入连接器上，使用控制策略引擎从控制策略解析模块获取当前被请求使用的数据产品所对应的一条或多条数据使用控制策略；
3. 校验使用策略：数据使用方接入连接器对使用策略中的约束条件、操作行为进行校验：
   a) 使用控制策略引擎从使用环境、信息提供组件中收集必要的上下文信息（如环境信息、操作者身份、连接器身份、操作类型、时间、地点、应用等）等，并进行策略中的约束条件进行判断；
   b) 使用控制策略引擎应对数据加工使用的所有相关的算法/模型/应用程序进行核验，确保其与使用策略中的操作行为保持一致；
4. 同步策略执行情况：数据使用方连接器将使用策略的校验结果和校验过程信息等同步给数据提供方，数据提供方的使用控制模块验证校验结果的真实性和完整性。根据数据提供方的要求，校验过程信息中可以包含环境信息、时间等上下文信息、算法/模型/应用程序信息，数据提供方可本地进行验证；
5. 数据交付：数据提供方数据使用控制模块验证核验结果的真实性和完整性后，根据策略中规定的数据交付方式，数据提供方接入连接器将数据产品交付至数据使用方接入连接器。当数据产品首次交付，或每次使用后要求被删除时，在之后的每次合规使用时数据提供方接入连接器均需执行交付操作；
6. 操作执行：在行为校验通过并完成额外操作（如有）后，接入连接器允许数据使用行为的实际执行，包括调用算法、运行模型、访问数据、用后删除等操作，期间进行持续监控和行为记录；
7. 记录存证：数据使用过程中，根据策略约定，会对数据的使用过程关键步骤进行记录存证；使用方接入连接器在任务完成后，生成履约证明（包括策略执行日志摘要、存证ID、区块链记录等），并发送给数据提供方接入连接器和服务平台，作为合约履行的最终凭证。

在数据使用过程中，数据使用方接入连接器与提供方接入连接器实时交互情况，包括实时运行状态、行为日志、策略校验结果等，若运行过程中在合约终止、策略失效、环境变更等异常情况下数据产品仍能被使用，数据提供方接入连接器可发起终止指令终止当前使用操作。

5.2.2 可信数据空间服务平台辅助接入连接器实现使用控制

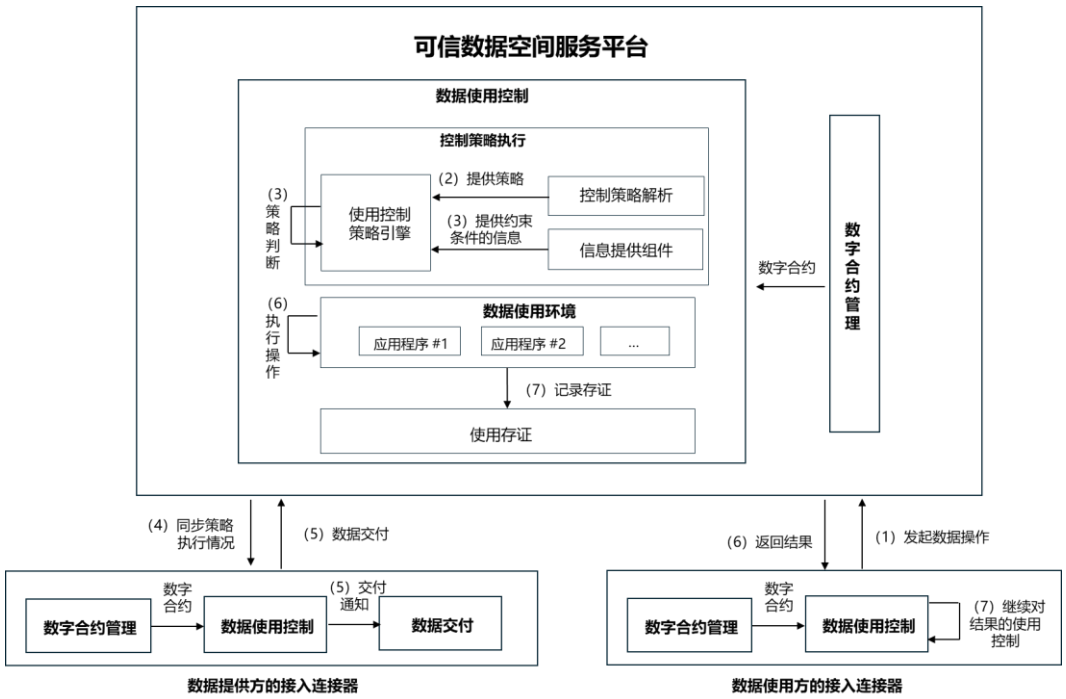

图4 可信数据空间服务平台和接入连接器的使用控制交互流程图

当接入连接器功能不足以满足数字合约预定的操作或约束条件，或两个异构接入连接器进行数据交互时，可信数据空间服务平台可为接入连接器提供集中式的使用控制环境，支持数据融合、联合建模等操作。数据提供方、数据使用方和数据服务方通过可信数据空间服务平台完成数字合约的签署，并由服务平台同步数字合约至各方接入连接器。数据使用控制模块中的控制策略解析模块从数字合约中解析出使用控制策略（操作行为和约束条件等）并安全保存，交互过程如下：

1. 发起数据使用操作：数据使用方接入连接器向可信数据空间服务平台发起数据使用操作，操作信息中包含数据产品、使用方式、使用者信息等；
2. 获取数据使用策略：在可信数据空间服务平台上，使用控制策略引擎从策略解析模块获取当前被请求使用的数据产品所对应的一条或多条数据使用控制策略；
3. 校验使用策略：可信数据空间服务平台对使用策略中的约束条件、操作行为进行校验：
   a) 使用控制策略引擎从使用环境、信息提供组件中收集必要的上下文信息（如操作者身份、连接器身份、操作类型、时间、地点、应用等）等，并进行策略中的约束条件进行判断；
   b) 使用控制策略引擎应对数据加工使用的所有相关的算法/模型/应用程序进行核验，确保其与使用策略中的操作行为保持一致；
4. 同步策略执行情况：可信数据空间服务平台将使用策略的校验结果和校验过程信息等同步给数据提供方，数据提供方的数据使用控制模块验证校验结果的真实性和完整性；根据数据提供方的要求，校验过程信息中可以包含环境信息、时间等上下文信息、算法/模型/应用程序信息，数据提供方可本地进行验证；
5. 数据交付：数据提供方数据使用控制模块验证核验结果的真实性和完整性后，根据策略中规定的数据交付方式，数据提供方接入连接器将数据产品交付至可信数据空间服务平台，当数据产

品首次交付，或每次使用后要求被删除时，数据提供方均需执行交付操作。若产品已在可信数据空间服务平台托管、缓存或加密留存，则无需数据提供方执行数据交付，可信数据空间服务平台经过权限验证后从缓存或加密存储介质中获取数据产品；

6. 操作执行：在行为校验通过并完成额外操作（如有）后，可信数据空间服务平台允许数据使用行为的实际执行，包括调用算法、运行模型、访问数据、用后删除等操作，期间进行持续监控和行为记录；数据结果以策略约定的方式提供给数据使用方接入连接器，使用方接入连接器将依据数据合约对结果数据的使用进行管控；
7. 记录存证：数据使用过程中，根据策略约定，会对数据的使用过程关键步骤进行记录存证。

6 功能要求

6.1 接入连接器

6.1.1 数据使用环境

6.1.1.1 软硬件环境

软硬件环境用于保障数据提供方数据产品在接入连接器内被可信使用，具体要求如下：

a) 运行环境：应支持根据策略要求构建多类型的运行环境；应具备隔离性，确保不同数据任务之间的资源与操作相互隔离；宜支持通过TPM、TEE等可信计算模块实现对运行环境的可信度量；
b) 存储环境：若策略中声明数据产品可落盘存储，则存储环境应具备访问隔离、权限控制、加密存储、存取审计等安全功能，确保数据产品在存储期间不被未授权访问、篡改或泄露，并保证数据产品与策略绑定；
c) 数据销毁：若策略中声明数据产品用后删除，则接入连接器应具备数据产品到期后的运行环境自动销毁数据能力，确保数据产品和中间数据不留存。

6.1.1.2 算法应用

接入连接器按需支持算法、模型或应用程序的管理、接入与运行，以实现对数据的分析、处理或计算，具体要求如下：

a) 算法支持：若策略中声明数据产品可被使用的算法，策略应配套约定算法输出是否可下载，可选择约定输入字段等策略；应确保所执行的算法与策略约定完全一致，如可在算法调用前校验算法唯一标识或比对算法信息；
b) 模型支持：若策略中声明数据产品可被应用的人工智能模型，应在模型调用前通过模型哈希校验、数字签名验证或模型注册信息比对等方式确保所使用的模型与策略声明一致；
c) 应用支持：若策略中声明数据产品在某应用程序内使用，数据使用方接入连接器应支持应用程序的隔离部署，支持部署后对应用程序进行可信签名验证，确保未经授权的应用不可使用数据产品。

6.1.1.3 使用监控

在接入连接器的数据运行环境内持续监控数据使用行为，为策略执行情况反馈、异常中止及履约证明提供支撑，具体要求如下：

a) 策略监控：应具备策略解析、行为校验、操作执行等策略全生命周期的监控和记录能力；
b) 行为监控：应实时监控数据使用行为，检测数据越权使用、违规使用，支持告警和强制中止。

6.1.2 控制策略执行

6.1.2.1 策略支持

接入连接器可支持策略的具体要求如下：

a) 数据交付策略：若策略中声明数据产品在被使用前的处理操作（如脱敏、加密、格式转换、清洗、采样等），数据提供方接入连接器应在数据交付前执行，脱敏算法应确保敏感数据不泄露；
b) 使用过程策略：若策略中声明数据仅可被查看，应确保仅授权用户能够查看数据，并支持通过权限管控、数据沙箱、密态计算等技术保证数据不被修改、复制、下载、分发和交易；若策略中声明数据可被复制，接入连接器应支持在复制过程中添加水印或标记；若策略中声明数据可被存档，接入连接器应确保存档数据符合指定的存储安全要求，且在存档后能按策略声明的时间要求访问或删除；若策略中声明数据可被分发，应在合约中明确分发对象，分发过程具备加密传输和身份验证机制，并记录分发过程；若策略中声明数据可被使用，连接器应确保仅经过授权的算法/模型/应用程序可对数据进行处理，确保所有操作都在受控环境中执行；
c) 通用约束策略：应支持时间、地点、主体、客体等通用约束类策略的解析、校验和执行，如通过白名单、规则匹配、属性校验等多种方式进行判断。

6.1.2.2 策略解析

策略解析是接入连接器对接收到的策略进行结构化理解与语义转化的过程，具体要求如下：

a) 完整性校验：应通过数字签名、校验码等方式对接收到的策略进行完整性校验，保证下发的策略没有被篡改，符合各参与方的预期；
b) 语法解析：应支持策略语法解析功能，可解析策略的语法结构判断元素是否完整和语法是否正确，存在错误时可及时提示错误信息；
c) 语义解析：应支持策略语义解析功能，可准确识别策略内容中的约束条件、行为和逻辑关系；
d) 冲突检测：应具备多个策略的冲突检测能力，如授权冲突、条件约束矛盾、范围不一致等；
e) 可执行格式：应支持将策略转化或映射为系统可理解、可执行的数据结构、中间表达或可执行指令，如JSON、XML等常见结构化策略描述语言；
f) 策略存储：应保存策略解析结果，确保存储过程的完整性和机密性。

6.1.2.3 行为校验

行为校验是在数据使用请求发生时，接入连接器基于解析后的策略和当前环境信息，对数据使用行为是否符合预设策略做出动态判定，并输出相应的决策结果或触发控制指令的过程，具体要求如下：

a) 信息获取: 应支持从身份认证模块、数据库、数据使用环境等组件动态获取策略评估所需的上下文信息，包括但不限于数据使用主体标识、数据产品标识、连接器标识、应用标识、操作类型、请求时间、地点、使用环境等；
b) 条件核验：应根据使用控制策略要求，对每次行为请求的操作和所有约束条件进行核验，确保所有条件均符合策略约定。约束的示例如附录A所示；
c) 校验结果：应基于各类条件判断输出一个明确的校验结果，并将核验结果同步给数据使用方包括“允许”、“有条件允许”、“拒绝”或“默认拒绝”。

6.1.2.4 操作执行

操作执行是指在行为校验后，接入连接器根据校验结果对数据使用请求实施控制操作和执行附加操作的过程，具体要求如下：

a) 允许操作：若策略决策结果为“允许”，则数据使用方在符合策略要求的数据使用环境中执行策略中规定的操作行为；

b) 有条件允许：若策略决策结果为“有条件允许”，系统应先执行前提条件。当前提条件执行后，再次执行行为校验；
c) 拒绝操作：若策略决策结果为“拒绝”，则本次数据产品操作无法进行；
d) 默认操作：若策略决策结果为“默认拒绝”，则本次数据产品操作无法进行；
e) 义务事项：若策略声明需要执行必要的额外前置、并行或后置操作，如向身份认证系统请求进行二次认证、添加数据水印、数据用后删除、过程通知等，则应严格保证操作的执行顺序；
f) 效果核验：应支持在数据使用、存储、删除等关键操作执行后进行效果核验，如数字合约到期后的数据产品和中间数据删除；
g) 异常解决：应提供使用过程的异常中止能力，在合约失效、异常识别等情况下能够及时中断正在进行中的数据使用行为，并能及时通知数据提供方；
h) 容错机制：宜具备操作执行过程中的异常处理机制，如认证、通知、上报等操作执行失败后的重试功能。

6.1.3 使用存证

使用存证是接入连接器在策略解析、行为校验及操作执行环节中记录并存储每一操作详细信息的功能，用于支撑后续回溯、分析和审计，具体要求如下：

a) 操作记录：应记录数据提供方和数据使用方间策略协商修改过程的信息，包括时间、参与方、修改前后的策略信息等；
b) 过程记录：应记录策略解析、行为校验和操作执行环节的情况，记录内容包括时间和结果；
c) 日志查询：应具备日志检索功能，允许根据策略ID、时间范围、操作主体、执行结果等至少一种条件对策略相关记录进行查询；
d) 存证上报：应支持定期将存证信息上报至可信数据空间服务平台。

6.2 可信数据空间服务平台

6.2.1 数据使用环境

6.2.1.1 软硬件环境

软硬件环境用于保障数据提供方数据产品在可信数据空间服务平台内被可信使用，具体要求如下：

a) 运行环境：应支持根据策略要求构建多类型的运行环境，如明文计算环境、数据沙箱环境或隐私计算环境、密态计算环境等；应具备隔离性，确保不同数据任务、算法、用户之间的资源与操作相互隔离；宜支持通过TPM、TEE等可信计算模块实现对运行环境的可信度量；
b) 存储环境：若策略中声明数据产品可落盘存储，则存储环境应具备访问隔离、权限控制、加密存储、存取审计等安全功能，确保数据产品在存储期间不被未授权访问、篡改或泄露，并保证数据产品与策略绑定；
c) 环境销毁：若策略中声明数据产品用后删除，则可信数据空间服务平台应支持数据产品到期后的运行环境自动销毁功能，确保数据产品和中间数据不被保留或复用。

6.2.1.2 算法应用

可信数据空间服务平台按需支持算法、模型或应用程序的管理、接入与运行，以实现对数据的分析、处理或计算，具体要求如下：

a) 算法支持：若策略中声明数据产品可被使用的算法，算法应在可信数据空间服务平台登记，包括名称、版本、来源签名、调用权限等，并具备唯一标识；策略应配套约定算法输出是否可下载，可选择约定输入字段等策略；

b) 模型支持：若策略中声明数据产品应用于指定的人工智能模型，模型应在可信数据空间服务平台登记，包括名称、版本、来源签名、调用权限等，并具备唯一标识；应在模型调用前通过模型哈希校验、数字签名验证或模型注册信息比对等方式确保所使用的模型与策略声明一致；

c) 应用支持：若策略中声明数据产品被指定应用程序使用，则应用程序应在可信数据空间服务平台登记；可信数据空间服务平台应支持应用程序的隔离部署，支持部署后对应用程序进行可信签名验证，确保未经授权的应用不可使用数据产品。

6.2.1.3 使用监控

在可信数据空间服务平台的数据运行环境内持续监控数据使用行为，为策略执行情况反馈、异常中止及履约证明提供支撑，具体要求如下：

a) 策略监控：应具备策略解析、行为校验、操作执行等策略全生命周期的监控和记录能力；

b) 行为监控：应实时监控数据使用行为，检测数据越权使用、违规使用，支持告警和强制中止。

6.2.2 控制策略执行

6.2.2.1 使用控制管理

可信数据空间服务平台负责定义和管理数据使用控制策略和策略模板，制定后的策略模板在数字合约内进行选择，具体要求如下：

a) 管理操作：应支持可信数据空间运营方新增、修改、删除、审核、启用和禁用各数据使用控制策略和策略模板；

b) 策略开发：应支持可信数据空间运营方开发策略，开发过程应配置策略名称、ID、描述、参数、类型、关联对象（如数据/操作事件/用户角色等）、执行动作（如允许/拒绝）、优先级等信息；

c) 模板制定：应支持可信数据空间运营方制定策略模板，模板内容包括约束类和行为类策略，可参考附录A；

d) 策略生成：应支持策略实例通过服务平台数字合约明确和接入连接器间的协商生成；

e) 策略下发：若策略是在服务平台的合约内生成，合约签订后可信数据空间服务平台按照NDI—TR—2025—02确定的数据交易控制指令流程和要求向数据提供方和使用方连接器下发数据交易控制指令，可信数据空间服务平台应基于业务需求对相关信息进行拓展，以支持数字合约执行所必需的使用控制策略下发；

f) 模板共享：宜具备可信数据空间服务平台内模板的导入与导出功能，实现来自不同可信数据空间策略模板的集成应用。

6.2.2.2 策略支持

可信数据空间服务平台可支持策略的具体要求如下：

a) 数据交付策略：若策略中声明数据产品在被使用前的处理操作（如脱敏、加密、格式转换、清洗、采样等），可信数据空间服务平台应在托管数据被使用前执行预处理操作，脱敏算法应确保敏感数据不泄露；

b) 使用过程策略：若策略中声明数据可被托管，可信数据空间服务平台应确保托管数据符合指定的存储安全要求，且托管数据仅能按策略声明的要求进行使用或删除；若策略中声明数据可被分发，应在合约中明确分发对象，分发过程具备加密传输和身份验证机制，并记录分发过程；若策略中声明数据可被使用，可信数据空间服务平台应确保仅经过授权的算法/模型/应用程序可对数据进行处理，确保所有操作都在受控环境中执行；若策略中声明多源数据联合开发，服

务平台应具备数据沙箱环境，确保各方仅能访问各自数据且保证数据安全，宜支持通过多方安全计算、联邦学习等隐私保护计算技术增强数据安全；

c) 通用约束策略：应支持时间、地点、主体、客体等通用约束类策略的解析、校验和执行，如通过白名单、规则匹配、属性校验等多种方式进行判断。

6.2.2.3 策略解析

策略解析是可信数据空间服务平台对接收到的策略进行结构化理解与语义转化的过程，具体要求如下：

a) 完整性校验：应通过数字签名、校验码等方式对数据提供方接收到的策略进行完整性校验，保证策略在下发过程没有被篡改；

b) 语法解析：应支持策略语法解析功能，可解析策略的语法结构判断元素是否完整和语法是否正确，存在错误时可及时提示错误信息；

c) 语义解析：应支持策略语义解析功能，可准确识别策略内容中的约束条件、行为和逻辑关系；

d) 冲突检测：应具备多个策略间的冲突检测能力，如授权冲突、条件约束矛盾、范围不一致等；

e) 可执行格式：应支持将策略转化或映射为系统可理解、可执行的数据结构、中间表达或可执行指令，如JSON、XML等常见结构化策略描述语言；

f) 动态适配：若多个接入连接器策略描述不一致，可信数据空间服务平台应提供跨接入连接器的策略动态适配能力，支持对多个策略进行自动解析和语义转换；

g) 错误处理：应提供解析过程中的错误处理功能，在解析失败或语义不明确时记录异常信息，支持触发告警或人工确认等处理方式；

h) 策略说明：可信数据空间服务平台宜提供策略内容的可视化解释界面或机器可读文档接口，包含字段含义、触发条件、受控资源与影响范围；

i) 解析存储：应保存策略解析结果，确保存储过程的完整性和机密性。

6.2.2.4 行为校验

行为校验是在数据使用请求发生时，可信数据空间服务平台基于解析后的策略和当前环境信息，对数据使用行为是否符合预设策略做出动态判定，并输出相应的决策结果或触发控制指令的过程，具体要求如下：

a) 信息获取: 应支持从身份认证模块、数据库、数据使用环境等组件动态获取策略评估所需的上下文信息，包括但不限于数据使用主体标识、数据产品标识、连接器标识、应用标识、操作类型、请求时间、地点、使用环境等；

b) 条件核验：应根据使用控制策略要求，对每次行为请求的操作和所有约束条件进行核验，确保所有条件均符合策略约定，约束的示例如附录A所示；

c) 校验结果：应基于各类条件判断输出一个明确的校验结果，包括“允许”、“有条件允许”、“拒绝”或“默认拒绝”。

6.2.2.5 操作执行

操作执行是指在行为校验后，可信数据空间服务平台根据校验结果对数据使用请求实施控制操作和执行附加操作的过程，具体要求如下：

a) 允许操作：若策略决策结果为“允许”，则数据使用方在符合策略要求的数据使用环境中执行策略中规定的操作行为；

b) 有条件允许：若策略决策结果为“有条件允许”，系统应先执行前提条件。当前提条件执行后，再次执行行为校验；

c) 拒绝操作：若策略决策结果为“拒绝”，则本次数据产品操作无法进行；
d) 默认操作：若策略决策结果为“默认拒绝”，则本次数据产品操作无法进行；
e) 义务事项：若策略声明需要执行必要的额外前置、并行或后置操作，如向身份认证系统请求进行二次认证、添加数据水印、数据用后删除、过程通知等，则应严格保证操作的执行顺序；
f) 效果核验：应支持在数据使用、存储、删除等关键操作执行后进行效果核验，如数字合约到期后的数据产品和中间数据删除；
g) 异常解决：应提供使用过程的异常中止能力，在合约失效、异常识别等情况下能够及时中断正在进行中的数据使用行为，并能及时通知数据提供方；
h) 容错机制：宜具备操作执行过程中的异常处理机制，如认证、通知、上报等操作执行失败后的重试功能。

6.2.3 使用存证

使用存证是可信数据空间服务平台在策略下发、策略解析、行为校验及操作执行环节中记录并存储每一操作详细信息的功能，用于支撑后续回溯、分析和审计，具体要求如下：

a) 操作记录：应记录策略制定、修改、删除、审核、启用、禁用等相关管理操作；
b) 过程记录：应记录策略下发、策略解析、行为叫和实施各环节的情况，记录内容包括时间和行为结果；
c) 日志查询：应具备日志检索功能，允许根据策略ID、时间范围、操作主体、执行结果等条件对策略操作进行查询；
d) 审计回溯：应支持策略下发、解析、行为校验、操作执行全过程的行为回溯，支持异常行为和特定数据对象、特定用户行为的分析。

7 使用控制接口规范

7.1 接口列表

表1 接口列表

序号	接口名称	接口编码	调用方	提供方
1	服务平台策略下发接口	/strategyIssuance	接入连接器	可信数据空间服务平台
2	策略执行情况反馈接口	/executionFeedback	可信数据空间服务平台、接入连接器	接入连接器
3	异常中止控制接口	/abnormalTermination	数据提供方接入连接器	数据使用方接入连接器
4	履约证明发送接口	/fulfillmentProof	接入连接器	接入连接器

7.2 接口要求

7.2.1 服务平台策略下发接口

可信数据空间服务平台按照NDI—TR—2025—02确定的数据交易控制指令获取流程和要求向接入连接器提供数据交易控制指令同步，并拓展使用控制策略相关内容。

表2 服务平台策略下发接口

接口名称	服务平台策略下发接口	StrategyIssuance

接口访问地址	/strategySend				HTTP Method	POST
功能						
请求参数：						
序号	参数名称	字段名称	数据类型	长度	可选/必选	说明
1	合约ID	contractId	string	36	必选	数字合约唯一标识
2	策略ID	strategyId	string	36	必选	策略实例唯一标识
3	策略版本	strategyVersion	string	36	必选	下发策略的版本号
4	交易合约控制指令	transactionExecutionStrategy	json	—	必选	示例见附录B
5	下发时间	issuedAt	string	—	必选	ISO8601 时间戳
6	平台签名	signature	string	—	必选	服务平台数字签名

7.2.2 策略执行情况反馈接口

将行为校验和操作执行的结果或异常信息反馈至数据提供方接入连接器或可信数据空间服务平台。

表3 策略执行情况反馈接口

接口名称	策略执行情况反馈接口				executionFeedback	
接口访问地址	/executionFeedback				HTTP Method	POST
功能						
请求参数：						
序号	参数名称	字段名称	数据类型	长度	可选/必选	说明
1	连接器ID	connectorId	string	36	必选	接入连接器唯一标识
2	合约ID	contractId	string	36	必选	数字合约唯一标识
3	策略ID	strategyId	string	36	必选	策略实例唯一标识
4	执行结果	result	string	—	必选	allowed/denied/conditional
5	执行时间	timestamp	string	—	必选	ISO8601 时间戳
6	详情	details	object	—	可选	执行上下文或错误信息
7	连接器签名	signature	string	—	必选	接入连接器数字签名

7.2.3 异常中止控制接口

当检测到合约或策略异常（如安全事件、合约失效），请求中止正在执行的使用控制流程。

表4 异常中止控制接口

接口名称	异常中止控制接口		abnormalTermination	
接口访问地址	/abnormalTermination		HTTP Method	POST
功能				

请求参数：						
序号	参数名称	字段名称	数据类型	长度	可选/必选	说明
1	中止请求ID	terminationId	string	36	必选	本次中止操作唯一标识
2	合约ID	contractId	string	36	必选	关联数字合约唯一标识
3	策略ID	strategyId	string	36	必选	策略实例唯一标识
4	中止原因	reason	string	256	必选	简要描述中止触发原因
5	触发方	triggeredBy	string	—	必选	provider/system
6	触发时间	timestamp	string	—	必选	ISO8601 时间戳

7.2.4 履约证明发送接口

在完整执行完数字合约后，数据使用方接入连接器将生成履约证明并发送给数据提供方接入连接器和可信数据空间服务平台。

表5 履约证明发送接口

接口名称	履约证明发送接口		fulfillmentProof	
接口访问地址	/fulfillmentProof		HTTP Method	POST
功能				
请求参数：				
序号	参数名称	字段名称	数据类型	长度	可选/必选	说明
1	证明ID	proofId	string	36	必选	本次履约证明唯一标识
2	合约ID	contractId	string	36	必选	关联数字合约唯一标识
3	策略ID	strategyId	string	36	必选	关联策略实例唯一标识
4	日志摘要	logHash	string	—	必选	执行日志的哈希摘要
5	区块链交易ID	blockchainTx	string	—	可选	存证上链交易ID
6	发送时间	timestamp	string	—	必选	ISO8601 时间戳
7	连接器签名	signature	string	—	必选	发送方数字签名

8 安全要求

8.1 使用环境安全

使用控制策略需要联动使用环境共同保证数据可控使用，使用环境的安全性直接影响使用控制技术的有效性，具体要求如下：

a) 环境隔离：应支持物理隔离、虚拟隔离及容器隔离等多种隔离方式，确保不同任务间的数据、内存、进程安全隔离；宜提供抵御来自管理员或高权限操作越权访问的措施；

b) 环境完整性：应支持在数据使用前对执行环境进行完整性验证；

c) 组件安全：应支持对部署在使用环境内的算法模型、应用程序、插件等进行可信认证或数字签名校验，确保其来源可信、内容未篡改；

d) 硬件保障：宜具备TEE、TPM等硬件实现数据使用过程中的计算和存储操作可信执行。

8.2 策略安全

8.2.1 核验安全

策略核验是数据使用前对所配置的使用控制策略进行完整性、合规性和有效性的校验，确保策略未被篡改、符合平台设定的规则，具体要求如下：

a) 策略合规：应在核验阶段对所配置的使用控制策略进行合规性核验，确保策略内容符合相关法律法规、行业规定及平台管理要求，禁止设置存在违规风险或超越授权范围的策略规则；
b) 过程安全：应保证核验过程的核验内容的完整性和真实性，避免策略在核验过程中受到篡改、伪造或绕过，如采用数字签名、存证、可信计算等技术手段；
c) 结果安全：应对核验结果进行完整性保护，确保策略核验结果在使用过程中不被非法修改。

8.2.2 传输安全

策略内容和执行情况记录会在可信数据空间服务平台和接入连接器间进行传输，传输过程的具体要求如下：

a) 身份认证：应在数据传输前对接入连接器的身份进行认证，确保接入连接器已注册且身份可信，如通过证书或密钥等方式认证；
b) 完整性：应采用校验技术或密码技术保证通信过程中数字合约和使用控制策略的完整性，确保传输过程不被篡改；
c) 保密性：应采用密码技术保证通信过程中数据和使用控制策略的保密性。

8.2.3 存储安全

数据产品和对应的使用控制策略会保存在可信数据空间服务平台或接入连接器中，用于后续调用、审计与追溯。为保障已存储策略的安全性和存储数据严格按策略调用，存储安全要求如下：

a) 策略绑定：应确保存储中的使用控制策略始终与其控制的数据产品绑定，保证数据与策略关联关系的一致性；
b) 内容防篡改：应具备使用控制策略的防篡改能力，确保策略内容在存储期间不被损坏或篡改，如通过完整性校验；
c) 保密性：宜采用密码技术保证数据和使用控制策略在存储过程中的保密性。

8.3 使用过程安全

使用过程安全是指在数据产品在被使用的过程中，确保其不会被非法访问、篡改、复制、泄露或偏离授权用途，具体要求如下：

a) 存储调用安全：应确保仅经过数据提供方授权的使用方可依据策略规则访问和使用已存储的数据；
b) 机密性保护：如果在数字合约中规定了机密性保护需求的高敏感数据，应确保计算过程中数据的机密性；应确保中间数据、计算结果不能被参与方、平台的内部人员（如运维人员、管理人员等）非授权获取或滥用；应保证计算结果的保密性，计算结果是加密处理的，仅有权限的参与方可解密。

8.4 日志存证安全

保障策略生成、下发、校验等全生命周期策略相关记录的完整性与安全性，具体要求如下：

a) 防篡改：应保证策略下发、策略解析、行为校验日志在记录、传输和存储过程时的不可篡改，如采用哈希校验、区块链、可信计算等技术；
b) 授权访问：应保证仅授权用户和审计方可访问策略相关日志；

c) 隐私保护：若存证日志中包含敏感字段（如数据标识、用户ID、模型调用信息等），应采用脱敏、匿名化等方式确保日志内的隐私信息不泄露；
d) 加密存储：宜采用加密技术对策略解析、决策、执行生命周期的日志进行存储，并结合密钥管理、访问控制等措施，确保数据在存储过程中的安全性；
e) 可信记录：宜对日志的生成、查看、转发等关键操作行为的操作者附加数字签名及时间戳信息；
f) 分布式存储：宜具备分布式存储和备份能力，支持将日志存证同步备份于可信数据空间服务平台系统内的多节点。

附 录 A
（资料性）
使用控制策略示例

表 1 策略说明

类别	维度	策略	说明
约束	时间	限定数据产品使用次数	数据产品在时间区间内最多可被使用的次数
		限定数据产品使用时间范围	对数据产品可使用的有效时间范围进行限定、仅允许在设定的时间范围内进行使用
		限定使用时间窗口及周期	在限定数据产品使用时间范围基础上，进一步规定数据产品使用的时间窗和周期，如：仅能在某天（周期）的特定时间段（窗口）内使用数据
		限定使用频率	对数据产品在时间区间内限制每分钟/小时/天的调用频率，防止批量滥用或攻击行为
	地点	限定地域	数据产品仅可在指定地理区域内使用
		限定网络地址	数据产品仅可通过特定标识的IP地址使用
		限定运行环境	数据产品使用的运行环境必须满足一定安全条件，如数据沙箱环境、可信执行环境等
	主体	限定交付连接器	数据产品仅可由特定标识或特定组织的接入连接器进行交付（标识信息遵循：数据基础设施 标识管理规范-NDI-TR-2025-04 标准约定）
		限定使用连接器	数据产品仅可在特定标识或特定组织的接入连接器上使用（标识信息遵循：数据基础设施 标识管理规范-NDI-TR-2025-04 标准约定）
		限定角色	数据产品仅可由数据使用方的特定角色或具有某类权限的用户使用
	客体	限定状态	数据在使用前需处于特定状态，如加密、匿名化等
		限定使用量	数据产品在时间区间内最大使用规模，如10G
		限定分发数据量	数据产品的分发数据量，包括单次分发量和总分发量
		限定字段	数据产品中仅部分字段可被使用
	通信	限定网络要求	数据产品仅可通过指定的VPN进行传输
		限定传输协议	数据产品仅可通过特定网络传输协议进行传输
		限定通信信道	数据产品的传输必须通过加密通道（不低于TLS 1.2）进行

	存储	限定存储方式	数据产品可持久化存储
		限定存储形式	数据产品应加密存储，并限定加密算法，如SM4、AES-256等
		限定存储位置	数据产品只能存储在指定位置，如特定接入连接器
		限定存储时长	数据产品在使用后最长可保留时间，到期应强制销毁
行为	操作	查看	数据产品可被用于查看
		复制	数据产品可被复制
		下载	数据产品可被下载到数据使用方本地
		数据处理	数据产品可被转换、脱敏操作
		联合开发	数据产品可被用于多使用方的联合开发
		分发	数据产品可被用于分发给除数据使用方外的第三方
		策略传递	数据分发给第三方前，必须附带原有使用控制策略
		出售	数据产品可被用于交易
		删除	数据产品到期或使用完成后立即删除
		应用程序	数据产品仅能被某些特定应用程序或工具调用
		算法	数据产品仅能被使用于某些特定算法，如预处理、分析、建模等
		机器学习模型	数据产品仅能被使用于某个特定机器学习模型进行模型训练或推理
		结果下载	基于数据产品加工、计算后的结果是否可下载到本地
		行为记录发送	数据产品使用行为记录将同步发送至数据提供方或上报至可信数据空间服务平台
		使用通知	数据产品在每次使用后通知提供者或指定方
		自定义	其他使用控制策略

附 录 B
（资料性）
交易合约控制指令示例

```
{
  // 交付信息
  "deliveryInfo": {
    // 数据传输模式，可选值：push / pull
    "transferMode": "pull"
  },

  // 使用控制策略
  "usageControlStrategy": {
    // 时间维度控制
    "time": {
      // 限定使用总次数
      "usageCountLimit": 1000,

      // 限定可使用的时间范围
      "validTimeRange": {
        "start": "2025-07-01T00:00:00Z",  // 起始时间
        "end": "2025-12-31T23:59:59Z"     // 结束时间
      },

      // 使用时间窗口与周期
      "timeWindow": {
        "days": ["Monday", "Wednesday", "Friday"], // 可使用的星期几
        "startTime": "09:00",  // 每天开始时间
        "endTime": "17:00"     // 每天结束时间
      },

      // 使用频率限制
      "frequencyLimit": {
        "perMinute": 10,  // 每分钟最大使用次数
        "perHour": 100,   // 每小时最大使用次数
        "perDay": 500     // 每天最大使用次数
      },

      // 限定使用的触发事件件
      "triggerEvents": ["taskCompleted", "externalSignal"]
    },

    // 地点/位置控制
```

```
"location": {
  // 限定使用地域（如行政区划码）
  "regionLimit": ["CN-Zhejiang", "CN-Beijing"],

  // 限定使用位置标识（平台或连接器）
  "positionLimit": ["connector-001", "platform-ABC"],

  // 限定运行环境（如沙箱、TEE）
  "environmentRequirement": ["sandbox", "TEE"]
},

// 主体控制
"subject": {
  // 限定允许使用的用户或组织
  "allowedUsers": ["org123", "user456"],

  // 限定交付连接器
  "deliveryConnectors": ["conn-789"],

  // 限定使用连接器
  "usageConnectors": ["conn-101"],

  // 限定角色（如数据服务方）
  "roleLimit": ["dataProvider"]
},

// 使用行为控制
"behavior": {
  // 限定用途（查看、处理等）
  "allowedPurposes": ["view", "process", "download"],

  // 限定调用应用程序
  "allowedApplications": ["appA", "toolB"],

  // 限定允许的算法类型
  "allowedAlgorithms": ["preprocess", "modeling"],

  // 是否允许结果下载
  "resultDownload": true,

  // 终止条件
  "terminationConditions": {
    "by": "consumer",        // 谁可以终止
```

```
    "when": "taskCompleted"  // 在什么条件下终止
  },

  // 是否记录并上报使用日志
  "sendUsageLogs": true,

  // 是否使用后通知提供者
  "notifyOnUse": true,

  // 是否强制传递原始策略
  "policyForwardingRequired": true
},

// 客体控制
"object": {
  // 限定数据状态（如加密）
  "requiredState": ["encrypted"],

  // 使用完成后立即销毁
  "autoDestroyAfterUse": true,

  // 最大访问数据量（如 10G）
  "maxAccessVolume": "10GB",

  // 最大分发量限制
  "maxDistributionVolume": {
    "single": "2GB",  // 单次
    "total": "20GB"   // 总量
  }
},

// 通信安全控制
"communication": {
  // 是否强制使用 VPN
  "requiredVPN": true,

  // 允许的传输协议
  "allowedProtocols": ["HTTPS", "MQTT"],

  // 加密信道要求
  "encryptedChannel": "TLS1.2+"
},
```

```
    // 存储策略控制
    "storage": {
      // 是否允许持久化存储
      "persistenceAllowed": false,

      // 存储加密要求
      "encryption": {
        "enabled": true,
        "algorithm": "SM4"
      },

      // 限定存储位置
      "storageLocation": ["connector-001"],

      // 存储最长保留时间（单位：天）
      "retentionTimeDays": 30
    },

    // 自定义策略
    "custom": {
      // 其他自定义使用控制策略
      "other": "自定义控制策略描述"
    }
  }
}
```

参 考 文 献

[1] 可信数据空间发展行动计划（2024—2028 年）（国数资源〔2024〕119号）
[2] 数据领域常用名词解释（第一批）（国家数据局）
[3] 数据领域常用名词解释（第二批）（国家数据局）