ICS 35.020
CCS L 80

团 体 标 准

T/CIIA 020—2022

科学数据 安全传输技术要求

Scientific data- Technical requirements of security transmission

2022－10－20 发布　　2022－10－20 实施

中国信息协会　　发 布

目　　次

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。

本文件由中国信息协会提出并归口。

本文件起草单位：中国科学院计算机网络信息中心、广州物联网研究院、精位大辰数字科技（厦门）有限公司、中国信息通信研究院、厦门帝嘉科技有限公司、华控清交信息科技（北京）有限公司、中国标准化研究院、中国科学技术信息研究所、中国电子技术标准化研究院、北京云迹科技股份有限公司、中国网络安全审查技术与认证中心、中国核动力研究设计院、深圳华大生命科学研究院、北京神州数码云计算有限公司、中国软件评测中心（工业和信息化部软件与集成电路促进中心）、北京声智科技有限公司、山东旗帜信息有限公司、北京山水云图科技有限公司、杭州半云科技有限公司、杭州默安科技有限公司、北京贵士信息科技有限公司、山东亿云信息技术有限公司、南京易科腾信息技术有限公司、四川赛闯检测股份有限公司、广州广电计量检测股份有限公司、江苏蓝创智能科技股份有限公司、福建福昕软件开发股份有限公司、北京浩瀚深度信息技术股份有限公司、中科柏诚科技（北京）股份有限公司、中运科技股份有限公司、杭州瑞成信息技术有限公司、航天云网科技发展有限责任公司、浙江云针信息科技有限公司、中电鸿信信息科技有限公司、淳安县数据资源中心、杭州市拱墅区数据资源管理局、北京滴普科技有限公司、北京网智易通科技有限公司、北京蓝象标准咨询服务有限公司。

本文件主要起草人：廖方宇、杜冠瑶、杜闽、魏金侠、吴灿金、赵静、龙春、胡良霖、靳晨、王志强、甘杰夫、朱艳华、支涛、景慧昀、陈孝良、李良、邱瀚、陈强、姜楠、陈细平、高瑜蔚、胡红亮、魏兴国、王建辉、吴士伟、晏志文、冯丽、黄跃珍、许晓耕、黄红娟、李坤、张释元、吴晓春、王德敬、张清枝、赵欢、徐春、金征雷、刘永进、王璐、肖赟、叶俊、韩志宏、姜云洲、吴小前、胡泊、周润松、谭雅熙、侯海宾、吴坚平、陈平、王道远、金岩、乔华阳、张德保、王新亮、马建红、段小莉。

本文件首次发布。

引　言

科学数据是科技创新的基础，其安全、合规、有序流动将是推动科学数据开放共享和创新应用的关键。科学数据也是重要的国家战略资源，保障科学数据在传输过程中的机密性、完整性、可用性具有非常重要的意义。而目前我国在科学数据管理上还存在一定不足，在科学数据的传输和共享环节缺少全面的标准指导。

本文件立足于现有的国内外科学数据传输标准和规定，旨在从科学数据安全传输需求出发，分别从科学数据分级和科学数据传输参与各方两个维度上对科学数据安全传输提出技术要求，在保障科学数据传输流程、技术、内容安全的同时，尽可能满足不同安全级别科学数据的传输安全需求。

本文件将为科研单位提供科学数据安全传输技术指导；为政府管理部门提供科学数据传输环节安全监管依据；为从事科学数据相关活动的公司提供技术执行和参照标准。

科学数据 安全传输技术要求

1 范围

本文件规定了科学数据传输参与各方在传输资质、传输技术、传输规程等方面的要求；对不同级别的科学数据规定了不同级别的安全要求。

本文件适用于从事科学数据相关活动有关数据传输过程中安全防护。

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 25069 信息安全技术 术语

GB/T 37964 信息安全技术 个人信息去标识化指南

3 术语和定义

GB/T 25069界定的以及下列术语和定义适用于本文件。

3.1

科学数据 scientific data

人类社会科技活动积累的或通过其他方式获取的反映客观世界的本质、特征、变化规律等原始性、基础性数据，以及根据不同科技活动需要进行系统加工整理的各类数据的集合。

[来源：GB/T 31075—2014，2.2.7]

3.2

数据传输 data transmission

数据从一个实体流动到另一个实体的过程。

[来源：GB/T 37988-2019，有修改]

3.3

科学数据传输 scientific data transmission

以科学数据为客体的数据传输活动。

3.4

传输安全 transmission security

保护网络中所传输信息的完整性、保密性、可用性及用户定制等特性。

[来源：GB/T 37025-2018，3.4]

3.5

科学数据安全分级 scientific data security grading

按科学数据的保密性、完整性、可用性及派生安全要求，经过一定程序的评估过程确定的科学数据安全等级。

3.6

科学数据供方 scientific data provider

按约定和规范生产和提供科学数据的组织机构、单位或个人。

3.7

科学数据需方 scientific data acquirer

按约定和规范接收和使用科学数据的组织机构、单位或个人。

3.8

隐私 privacy

个人所具有的控制或影响与之相关信息的权限，涉及由谁收集和存储、由谁披露。

[来源：GB/T 25069-2010，2.1.63]

3.9

信任 trust

在两个实体和/或元素之间，由一组活动和某一安全策略组成的如下关系：元素x信任元素y，当且仅当x确信y会以一种良好界定的方式（关于各项活动）行事，不会违反给定的安全策略。

[来源：GB/T 25069-2022，3.671]

3.10

可用性 availability

可由经授权实体按需访问和使用的性质。

[来源：GB/T 25069-2022，3.345]

3.11

完整性 integrity

数据所具有的特性，即无论数据形式作何变化，数据的准确性和一致性均保持不变。

[来源：GB/T 25069-2022，3.574，有修改]

3.12

保密性 confidentiality

信息对未授权的个人、实体或过程不可用或不泄露的性质。

[来源：GB/T 25069-2022，3.41]

4 安全传输技术要求分级

4.1 总体要求

科学数据安全传输技术要求应视具体情况而定。传输不同级别的科学数据时，应实施不同的安全技术要求。

4.2 分级

根据4.1分级总体要求，安全传输技术要求分为基本级和增强级两类。

a) 基本级：处理一般性科学数据传输应满足基本级安全传输技术要求。基本级主要针对一般性科学数据传输场景中，非加密环境下科学数据传输安全问题提出的基本技术要求；

b) 增强级：处理重要科学数据、敏感科学数据，涉及重大安全问题的科学数据传输应满足增强级安全传输技术要求，或参考等级保护或其他相关标准中安全等级划分内容；

c) 当不确定科学数据属于哪个级别时，宜参照增强级安全传输技术要求。

5 总则

科学数据传输过程中，科学数据将在供方和需方之间流通。科学数据供方将生产、使用或存储的科学数据传输至科学数据需方；科学数据需方从科学数据供方接收科学数据进行使用或存储。常见的科学数据传输场景见附录A。

相对于基本级安全技术要求，增强级还应满足更高的安全技术要求。

6 基本级安全技术要求

6.1 传输完整性

科学数据传输应保证数据完整性，应支持数据完整性校验机制，保证数据传输完整性。

6.2 传输可用性

科学数据传输应保证数据可用性，应符合下列要求：

a) 应选择可靠的网络链路、关键网络设备等，从而保证数据传输过程的稳定性、可靠性、时效性；
b) 在传输的数据有误时，应采取应对机制保证传输数据的准确性或正确性。

6.3 传输隐私

科学数据传输时，对于涉及个人信息、商业机密等的敏感数据，不应以明文形式传输，应采用如数据脱敏、数据加密、去标识化、差分隐私、多方安全计算等技术处理后才可传输，信息去标识化应符合GB/T 37964的要求。

6.4 传输信任

数据传输应符合下列信任要求：

a) 应采用加密算法、数字签名、密码校验等技术对传输双方的身份进行验证，保证数据来源与去向的正确性；
b) 应使用可信任介质进行传输；
c) 应在传输双方端到端之间提供一条通信传输路径，逻辑上与其他通信路径隔离，以保护数据免遭窜改或泄露。

6.5 传输协议

科学数据传输时，所使用的传输协议应支持数据完整性校验，保证传输可用性。此外，应符合下列要求：

a) 在使用自定义协议时，数据摘要、签名等密码算法应符合国家或行业相关标准要求；
b) 应定期审定、更新数据传输的保密协议。

6.6 日志与审计

科学数据传输应记录必要的日志并进行审计，应对每一次传输活动记录日志和审计。应符合下列要求：

a) 日志应记录科学数据传输的日期与时间；
b) 日志应记录科学数据传输的双方身份；
c) 日志应记录传输的科学数据大小、类型；
d) 日志应记录科学数据的传输方式；
e) 日志应记录传输的科学数据字节数；
f) 日志应记录传输是否成功。

7 增强级安全技术要求

7.1 传输完整性

符合6.1的要求。在数据完整性遭到破坏时，应恢复或重新获取数据。

7.2 传输可用性

符合6.2的要求。同时应使用冗余传输通道传输数据，必要时部署安全设备，保证传输通道高可用。

7.3 传输保密性

增强级科学数据传输应具有保密性，包括但不限于：

a) 应具有密码算法配置、密钥存储配置、密钥更新频率配置、密钥交换协议配置等密钥管理措施；
b) 所使用的密码技术应符合国家或行业相关标准要求。

7.4 传输隐私

符合6.3的要求。同时所使用的脱敏算法和去标识化处理应保证处理过程不可逆。

7.5 传输信任

符合6.4的要求。同时应采取措施确保端到端有一条专门的可信通信路径传输科学数据。

7.6 传输协议

符合6.5的要求，同时还应符合下列要求：

a) 使用的协议应保证数据保密性；
b) 应使用随机化的、隐蔽的传输协议；
c) 使用的协议应保证数据传输可靠性；
d) 使用的协议应具有容错性。

7.7 日志与审计

符合6.6的要求。同时还应符合下列要求：

a) 传输前应签订电子合约，交由各方签名确认；
b) 日志应记录传输过程中的异常事件；
c) 应对安全策略、传输协议更改活动记录日志和审计；
d) 应采取访问控制、日志清理、日志备份与复原等措施，对日志进行管理；
e) 对日志应采用数字签名技术，防止日志的伪造和窜改。

7.8 传输策略

增强级科学数据传输应具有安全策略，包括但不限于：

a) 具有监控传输流量的方法；
b) 具有监控并切断非法连接的策略；
c) 具有控制传输速率的策略。

8 传输各方安全要求

8.1 概述

本文件根据在科学数据传输活动过程中所扮演角色的不同，将参与传输活动的各单位划分为科学数据供方和科学数据需方。为保障传输安全，本章对各方的传输资质和传输规程规定特定的安全要求。

8.2 科学数据供方要求

8.2.1 传输资质

科学数据供方可传输的科学数据应与其资质相匹配，应符合下列要求：

a) 需传输基本级科学数据的单位，应无违法违规记录，且遵循学术诚信原则，无不良学术行为记录；
b) 需传输增强级科学数据的单位，应根据具体传输范围获得相关科研单位的授权；此外，涉及重要数据、敏感数据的传输，应获得科学数据中心或相关主管部门的授权；
c) 需要传输增强级科学数据的单位，涉及重要数据、敏感数据的传输，应主动确认需方获得科学数据中心或相关主管部门的授权。

8.2.2 传输规程

科学数据供方与科学数据需方进行数据传输时，应符合下列规程。

a) 传输前：
   1) 应检查对方是否具备接收待传输数据的资质；
   2) 应核实对方获取数据的目的、范围、频度、时效等；
   3) 应对敏感数据进行加密或脱敏处理，确保隐私安全；
   4) 预处理待传输数据，应保障数据质量，保障数据可用性。
b) 传输时：应与科学数据需方共同协商传输技术，传输技术应符合第 6 章和第 7 章的安全要求。
c) 传输后：应对此次传输活动生成的日志进行持久性保存与审计。

8.3 科学数据需方要求

8.3.1 传输资质

科学数据需方可接收的科学数据应与其资质相匹配，应符合下列要求：

a) 需接收基本级科学数据的单位，应无违法违规记录，且遵循学术诚信原则，无不良学术行为记录；
b) 需接收增强级科学数据的单位，应获得科学数据供方的授权；此外，涉及重要数据、敏感数据的传输，应获得科学数据中心或相关主管部门的授权。

8.3.2 传输规程

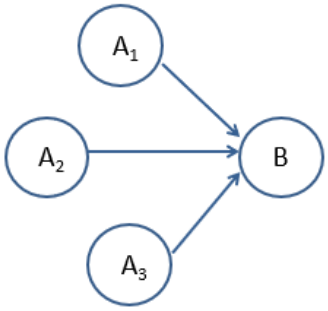
科学数据需方从供方或托管平台进行数据传输时，应符合下列规程。

a) 传输前：
   1) 应检查对方是否具备提供待传输数据的资质；
   2) 若从科学数据供方接收增强级数据，应获得科学数据供方授权。
b) 传输时：应与科学数据供方共同协商传输技术，传输技术应符合第 6 章和第 7 章的安全要求。
c) 传输后：应对此次传输活动生成的日志进行持久性保存与审计。

附 录 A
（资料性）
常见的科学数据传输场景

常见的科学数据传输场景见表A.1。

表A.1 科学数据传输场景

模型名称	传输模型	说明
传统模式		“传统模式”下的科学数据传输只涉及一个供方和一个需方。
新型模式		“新型模式”下的科学数据传输可能涉及多个供方和一个需方。

参 考 文 献

[1] GB/T 25069—2010 信息安全技术 术语
[2] GB/T 25069—2022 信息安全技术 术语
[3] GB/T 31075—2014 科技平台 通用术语
[4] GB/T 35294—2017 信息技术 科学数据引用
[5] GB/T 37025—2018 信息安全技术 物联网数据传输安全技术要求
[6] GB/T 37932—2019 信息安全技术 数据交易服务安全要求
[7] GB/T 37988—2019 信息安全技术 数据安全能力成熟度模型
[8] GB/T 38675—2020 信息技术 大数据计算系统通用要求
[9] 科学数据管理办法，国办发〔2018〕17号
[10] 中国科学院科学数据管理与开放共享办法（试行），中国科学院，2019年2月11日
[11] 中国科学院数据应用环境建设与服务 数据服务指导规范，中国科学院数据应用环境建设和服务项目组，2009
[12] 柏永青，杨雅萍，孙九林.国内外科学数据管理办法研究进展[J].农业大数据学报,2019,1(03):5-20+4