ICS 35.030
CCS L 80

T/CSAS

团　　体　　标　　准

T/CSAS 0004—2025

数据安全传输技术要求

Technical requirements for security transmission of data

2025-05-23 发布　　2025-07-01 实施

四川省网络空间安全协会　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。

本文件由四川省网络空间安全协会提出并归口。

本文件起草单位：中国电子科技集团公司第三十研究所、四川大学、豪符密码检测技术（成都）有限责任公司、成都墨甲信息科技有限公司、成都信息工程大学、成都理工大学、全域数据信息安全重点联合实验室西南实验室。

本文件主要起草人：张位、周阳、王瑶、李贝贝、冉桐、陈万钢、王杨、李佳琦、李林静、白杨、邢高杰、李冬芬、余展、赖一阳、陈薪鹏（排名不分先后）。

引　言

随着信息技术的飞速发展，计算机网络已成为数据交换和信息流通的重要基础设施。在数据驱动的社会经济背景下，数据的安全传输显得尤为重要。数据的非法获取、篡改或泄露不仅会对个人隐私和财产安全构成威胁，还可能对国家安全、社会稳定及经济发展产生深远影响。因此，制定一套科学、规范、全面的数据安全传输技术要求，对于保障数据在传输过程中的保密性、完整性、可用性等特性具有重要意义。

《数据安全传输技术要求》团体标准旨在通过详细规定计算机网络环境下数据传输的策略、协议、通道、加密等方面的技术要求，为不同级别的数据提供差异化的安全保护。具体而言，标准涵盖了从基本的数据传输安全策略到高级的加密技术和监控审计措施，以应对不同安全需求和数据敏感程度。同时，通过引用国家及行业相关标准，确保本技术要求的权威性和适用性。

在数据安全传输过程中，数据的划分和分级原则是基础。本文件依据数据的敏感度及潜在危害程度，将数据从低到高分为一般数据、重要数据和核心数据，并针对不同级别的数据提出相应的安全传输技术要求。这不仅有助于合理分配安全资源，还能在保障数据安全的前提下，提高数据传输的效率和灵活性。

此外，本文件还强调了数据传输的保密性、完整性、可用性及信任等方面的要求。通过要求采用先进的加密算法、安全传输协议和身份认证技术，确保数据在传输过程中不被非法访问、篡改或泄露。同时，要求建立可信传输路径和完善的监控审计机制，提高数据传输的可靠性和安全性。

总之，《数据安全传输技术要求》团体标准的制定，是应对当前数据安全挑战、保障数据在传输过程中安全性的重要举措。本文件将为计算机网络环境下的数据安全传输提供有力的技术支撑和保障，促进数据的安全、合规、高效流通。

数据安全传输技术要求

1 范围

本文件规定了通过计算机网络进行数据传输时，参与各方在传输策略、传输协议、传输通道等方面的要求；对不同级别的数据规定了不同级别的安全传输技术要求。

本文件适用于依托计算机网络进行数据安全传输的技术要求。

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 37025—2018 信息安全技术 物联网数据传输安全技术要求

GB/T 36322—2018 信息安全技术 密码设备应用接口规范

GB/T 37964—2019 信息安全技术 个人信息去标识化指南

GB/T 37988—2019 信息安全技术 数据安全能力成熟度模型

GB/T 25069—2022 信息安全技术 术语

GB/T 43697—2024 数据安全技术 数据分类分级规则

GM/T 0005—2021 随机性检测规范

T/CIIA 020—2022 科学数据 安全传输技术要求

T/CSAS 0001—2025 数据生命周期安全参考框架

3 术语和定义

GB/T 37988—2019、GB/T 25069—2022、GB/T 37025—2018、GB/T 5271.8—2001和GB/T 36322—2018界定的以及下列术语和定义适用于本文件。

3.1

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—2019，5.4.1，有修改]

3.2

安全 security

对某一系统，具有获得保密性、完整性、可用性、可核查性、真实性以及可靠性的性质。

[来源：GB/T 25069—2022，3.1]

3.3

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]

3.4

数据发送方 data sender

按约定和规范生产和提供数据的组织机构、单位或个人。

3.5

数据接收方　data receiver

按约定和规范接收和使用数据的组织机构、单位或个人。

3.6

数据完整性　data 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 5271.8—2001，08.01.07]

3.7

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]

3.8

加密　encipherment/eneryption

对数据进行密码变换以产生密文的过程。

[来源：GB/T 36322—2018，3.5]

3.9

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]

3.10

加密算法　encryption algorithm

将明文转换为密文的算法。

[来源：GB/T 25069—2022，3.280]

4　数据安全传输概述

4.1　数据安全传输

数据安全传输是指通过采取必要措施，确保数据在传输阶段，处于有效保护和合法利用的状态，以及具备保障持续安全状态的能力。

4.2　数据划分

依据GB/T 43697—2024《数据安全技术　数据分类分级规则》，从安全的角度将数据从高到低分为核心数据、重要数据、一般数据。核心数据是指对领域、群体、区域具有较高覆盖度或达到较高精度、较大规模、一定深度的，一旦被非法使用或共享，可能直接影响政治安全的重要数据，主要包括关系国家安全重点领域的数据，关系国民经济命脉、重要民生、重大公共利益的数据，经国家有关部门评估确定的其他数据；重要数据是指特定领域、特定群体、特定区域或达到一定精度和规模的，一旦被泄露或篡改、损毁，可能直接危害国家安全、经济运行、社会稳定、公共健康和安全的数据，仅影响组织自身或公民个体的数据一般不作为重要数据；一般数据为核心数据和重要数据之外的其他数据。

4.3　安全传输分级原则

根据4.2数据划分原则，不同类型的数据需要采取不同的安全传输技术要求。本文件将安全传输技术要求划分为基本级和增强级两类，具体如下：

a） 基本级：处理一般数据应满足基本级数据安全传输技术要求。基本级主要针对一般数据传输场景中，非加密环境下数据传输安全问题提出的基本技术要求；
b） 增强级：处理重要数据、核心数据应满足增强级数据安全传输技术要求。

注：不确定数据属于哪个级别时，宜参照增强级安全传输技术要求。

5 基本级数据安全传输技术要求

5.1 数据安全传输策略

具有正式、合法、合规、有效的传输策略程序以及控制措施，确保数据传输过程中的安全，且应满足如下要求：

a） 能清晰界定哪些信息可以明文传输，以及其所属的类别和范围；
b） 对于需要加密传输的敏感数据，例如：个人身份信息、生物特征信息、账号密码、密钥等，需制定可以采取的加密传输程序，包括选择合适的加密算法和密钥管理方法。

5.2 数据安全传输保密性

为确保数据在传输过程中的保密性，应满足如下要求：

a） 应使用安全传输协议（如HTTPS、TLS 1.2及以上版本）对网络传输的通信信道进行加密，确保通信信道的安全性；
b） 安全传输协议使用的加密算法应足够安全，密钥的安全强度至少为112比特〔如AES128、3DES（3个密钥的3DES）、SM4〕；
c） 加解密操作不能对系统性能造成过大的影响，导致传输延迟过高或影响其他业务的正常运行，加解密算法能够减少数据使用的等待时间，提高系统的整体效率；
d） 应具备基本的密钥管理策略，确保密钥不被明文存储，防止未经授权的访问或窃取，并定期更换密钥；
e） 数据安全传输使用的密码算法、密码技术、密码产品、密码服务等应遵循密码相关国家标准和行业标准。

5.3 数据安全传输完整性

能够基本确保数据在传输过程中不被非法损坏和篡改，保持数据的一致性，且应满足如下要求：

a） 应采用安全传输协议（如HTTPS、TLS 1.2及以上版本）对网络传输的通信信道进行完整性保护，确保通信信道的安全性；
b） 安全传输协议使用的杂凑算法应足够安全，密钥的安全强度至少为112比特〔如SHA256、SM3〕；
c） 数据安全传输完整性保护使用的密码算法、密码技术、密码产品、密码服务等应遵循密码相关的国家标准和行业标准。

5.4 数据安全传输可用性

确保合法用户能够持续访问和使用数据；在数据传输过程中，必须避免过多延迟，确保数据迅速到达目的地；系统应具备在数据传输过程中出现轻微错误时的自动恢复能力或提示数据发送方重新传输的机制。具体应满足如下要求：

a） 应采用访问控制技术以及针对关键链路采用冗余技术设计等手段增强数据访问的可靠性和鲁棒性；
b） 优化网络架构以减少中转节点，选择可靠的、有效的网络链路，使用低延迟传输协议〔如QUIC〕；

c) 在数据传输过程中出现轻微错误时，系统应自动检测并尝试恢复，并向数据发送方和数据接收方提供详细的错误日志和用户提示，便于数据发送方手动重传数据。

5.5 数据安全传输信任

数据安全传输应确保只有获得授权的用户能够访问和传输数据，并在数据传输之前保证主体对客体的身份信任，建立可信传输路径，且应满足如下要求：

a) 采用用户密码认证时，密码应包含大小写字母、数字和特殊字符，密码长度应达到一定的要求，并要求用户定期更新密码，以增加密码破解的难度；
b) 使用安全的加密算法、哈希函数、数字签名、认证协议等安全技术对数据传输方和数据接收方的身份进行验证，确保认证过程的安全性以及数据来源与去向的正确性；
c) 身份认证技术应简单易用，同时保持高安全性（例如单点登录SSO、生物特征识别），方便传输双方进行身份验证；
d) 在认证过程中，应清晰展示认证状态和认证结果，提高用户的安全感；
e) 在数据发送方和数据接收方端到端之间提供一条通信传输路径，此路径与其他通信路径逻辑上隔离，以保护数据免遭篡改或泄露。

5.6 数据安全传输协议

能够依托有效技术手段和管理措施，确保数据在传输过程中的安全性、完整性和可用性，同时优化协议性能和可扩展性，以适应不同应用场景的需求，且应满足如下要求：

a) 协议具有高可用性的冗余机制，确保在遭遇网络故障或流量激增时，数据传输依然保持稳定；
b) 协议支持多种数据格式和传输方式，以便灵活适应不同应用场景和业务需求的变化，确保系统的长期可维护性和扩展性。

5.7 数据安全传输通道

传输通道应具有一定的稳定性和可靠性，尽量减少数据传输中断的情况，且应满足如下要求：

a) 确保数据传输通道的物理安全，采取多层次的防护措施，如物理隔离、定期审计等；
b) 传输通道内具有基本身份认证措施，以确保通信双方的身份真实可靠。

5.8 数据安全传输防泄露

为防止数据传输过程中发生泄露，应满足如下要求：

a) 数据在传输过程中应采用加密技术，以防止数据在传输过程中被未授权方截获和读取。加密算法的选择应满足行业标准和法律法规的要求，确保加密强度足够高，以抵御常见的攻击手段；
b) 对数据传输过程中经过的中间节点（如路由器、交换机等）进行安全防护，确保这些节点的软件和硬件没有安全漏洞，防止攻击者利用中间节点窃取或篡改数据；
c) 对数据的发送方和接收方进行身份验证，确保双方的身份真实可靠。可以采用多种身份验证方式，如密码、数字证书、指纹识别、面部识别等，多因素身份验证能大大提高身份验证的安全性；
d) 在数据传输过程中，建立安全的会话机制，对会话进行加密和认证，防止会话劫持和中间人攻击；
e) 在数据传输和存储过程中，应实施数据完整性校验机制，以确保数据在传输或存储过程中未被篡改或损坏。

5.9 数据安全传输差错控制与纠错

具备简单的检错编码（如奇偶校验码、循环冗余校验码）和重传机制来确保数据的完整性和准确性。

5.10 数据安全传输监控与审计

不需要监控与审计。

6 增强级数据安全传输技术要求

6.1 数据安全传输策略

在满足基本级的基础上，应满足如下要求：

a) 策略和程序具有严格的权限管理机制，能够进行多种身份验证方式，确保仅授权人员可以进行信息传输操作；

b) 策略和程序能够对传输过程进行实时监测，及时发现异常并采取有效的预警和响应处置措施。

6.2 数据安全传输保密性

在满足基本级基础上，应满足如下要求：

a) 应对管理数据、鉴别信息、敏感信息、重要业务数据等重要数据进行应用层的信源加密，确保数据在发送端加密，并仅在接收端解密，防止中间节点访问数据，保障数据在整个传输过程中的保密性；

b) 密钥管理安全应符合以下要求：

1) 密钥的生成应通过密码检测认证的密码部件或模块内部产生，私钥和对称密钥的生成及协商应使用符合 GM/T 0005 要求的随机数；

2) 对称密钥和私钥应以安全形式或密文形式存储；

3) 若涉及密钥分发过程，应具备安全措施保证密钥真实性、保密性以及分发密钥的完整性；

4) 密钥应采取加密或知识拆分等安全方式进行导入导出；

5) 密钥应具有明确用途，密钥使用过程中应有相应安全措施，防止未经授权的访问、使用和篡改；

6) 若支持密钥备份与恢复，应以安全形式或密文形式备份到安全存储介质中，应支持以安全形式恢复备份的密钥，密钥备份或恢复应进行记录并生成审计信息；

7) 若涉及密钥归档过程，应使用有效的安全措施，保证归档密钥的安全性和正确性。归档密钥应只能用于解密该密钥加密的历史信息或验证该密钥签名的历史信息；密钥归档应进行记录并生成审计信息；密钥归档应进行数据备份，并使用有效的安全保护措施；在密钥生命周期结束、发生泄露或有泄露风险时应支持密钥销毁。

6.3 数据安全传输完整性

在满足基本级基础上，应满足如下要求：

a) 应对重要数据进行应用层的完整性保护，采用消息鉴别码机制、数字签名对管理数据、鉴别信息、敏感信息、重要业务数据等重要数据进行完整性保护，能够基本确保数据在传输过程中不被非法损坏和篡改，保持数据的一致性；

b) 应具有数据完整性的校验机制，确保数据一旦被损坏和篡改，能及时发现。

6.4 数据安全传输可用性

在满足基本级基础上，应满足如下要求：

a) 系统具备数据传输零中断能力，确保数据传输过程中出现任何中断情况时能够采取一定措施恢复传输能力。系统应采取包括但不限于冗余路径、自动重传机制、支持多通道传输、负载均衡等措施，系统能够在主路径发生故障时，自动切换至备用路径，降低因单点故障导致的中断风险，必要时部署安全设备（如防火墙、入侵检测系统等），保证传输通道高可用；

b) 系统应具有完善的监控机制，能够实时检测和评估数据传输的状态，包括发送速率、接收速率、丢包率等关键指标。当数据传输发生中断等异常情况时，系统能够迅速识别并及时向用户发送告警信息，以便用户能够快速采取相应措施。

6.5 数据安全传输信任

在满足基本级基础上，应满足如下要求：

a) 除用户名和密码外，还要求提供额外的认证因素，包括但不限于手机验证码、指纹识别、面部识别等，以提高认证的安全性，增强用户数据的保护力度，并提升用户对系统安全性的信任感；
b) 支持认证协议的升级和更新，这一功能包括但不限于协议版本管理、安全补丁及时应用，系统能够自动检测和识别当前使用的认证协议版本，并在新版本发布时提供升级服务；
c) 采用具有双向认证机制的安全认证协议（如TLS或SSL），不仅要求用户验证服务器的身份，还要求服务器验证用户的身份，以防止中间人攻击。在实现双向认证的同时，优化用户体验，确保认证过程便捷而不繁琐，以提高用户的接受度和满意度。

6.6 数据安全传输协议

在满足基本级基础上，应满足如下要求：

a) 协议具备防止数据被窃取、篡改、伪造的能力；
b) 协议具备错误处理和恢复机制，当数据传输出现问题时，能够进行相应的处理，保证数据传输的可靠性；
c) 协议具备通过校验、循环冗余检查等措施来识别数据损坏或丢失的能力；
d) 协议能够记录传输日志和状态信息，确保在出现问题时能够迅速采取相应的补救措施。

6.7 数据安全传输通道

在满足基本级基础上，应满足如下要求：

a) 传输通道具备精细的访问控制策略，以全面保障重要数据和核心数据的安全性；
b) 定期进行权限审计，检查并更新用户权限，及时撤销不再需要的访问权限，降低潜在的安全风险；
c) 建立专用监控和管理系统，对其性能和状态进行实时监测和预警，并提供详细的日志记录功能，帮助后续的故障排查和性能评估。

6.8 数据安全传输防泄露

在满足基本级基础上，应满足如下要求：

a) 具有强度更高的加密算法和技术，除了对称加密算法，可能还会结合非对称加密算法（如RSA）等，确保数据的保密性；
b) 能够实时监测数据传输情况，一旦发现数据泄露，能及时发出警报并采取相应的应对措施。

6.9 数据安全传输差错控制与纠错

在满足基本级基础上，应满足如下要求：

a) 具有较强的差错控制与纠错能力，能够利用更为复杂、有效的校验算法，来确保数据传输的完整性；
b) 能够在数据传输的多个环节进行验证，包括发送端、传输过程中和接收端，以确保数据在每个阶段都保持完整。

6.10 数据安全传输监控与审计

数据传输过程中的监控与审计应满足如下要求：

a） 监控与审计应涵盖数据传输过程的全生命周期；

b） 监控与审计内容应涵盖数据的加密情况、传输协议的安全性以及访问控制的有效性等方面。同时，还应对数据传输过程中的异常行为进行监控和记录，以便及时发现潜在的安全威胁；

c） 审计记录应妥善保存，防止被篡改或删除。