ICS 33.050
CCS M 30

团　体　标　准

T/TAF 101.3-2021

冷链物流可信溯源服务技术要求　第3部分：信息系统安全

Trusted and traceable service technical requirement for the cold chain logistics—Part 3: Information system security

2021-12-13 发布　　2021-12-13 实施

电信终端产业协会　发布

目　　次

前言 II
引言 III
1 范围 1
2 规范性引用文件 1
3 术语和定义 1
4 缩略语 1
5 信息系统安全要求 2
5.1 鉴权与安全防护要求 2
5.2 软件安全要求 2
5.3 数据安全要求 3
5.4 通信安全要求 3
5.5 个人隐私信息安全要求 3
5.6 系统审计安全要求 3
附录 A（规范性）冷链物流追溯信息内容 5
附录 B（规范性）特定物品冷链物流追溯信息内容 6

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。

本文件由电信终端产业协会提出并归口。

本文件起草单位：百度在线网络技术（北京）有限公司、中国信息通信研究院、联想（北京）有限公司、郑州信大捷安信息技术股份有限公司、四川长虹电子控股集团有限公司、青岛海信通信有限公司。

本文件主要起草人：王海棠、郭建领、吴月升、国炜、徐晓娜、李汝鑫、林巍巍、康亮、刘献伦、刘为华、黄德俊、罗阿文、郑梁、高仁忠。

引　言

信息系统是冷链业务信息流的关键载体，从企业核心的企业资源计划（ERP）系统到过程管理的订单管理系统（OMS）、仓库管理系统（WMS）、运输管理系统（TMS）与结算管理系统（BMS），信息系统对冷链物流业务起着非常重要的支撑作用。但冷链物流是长链条场景，在整个作业过程中会涉及多类数据的存储与访问需求，更会对接不同厂商、不同品牌、不同语言、不同架构、不同服务目标的信息系统，因此为完善冷链物流长链条服务的可拓展性、流畅性、流转数据的安全性以及提供完整的信息可溯源目标，就需要规范和约束数据传输、存储、访问、共享的技术要求，落实冷链物流过程中数据产生到消亡的安全管控，实现可鉴权、可接入、可存储、可查询、可留痕、可分析、可共享的管理目的。

因此，建议开展信息系统安全要求标准的立项，且该标准会作为冷链物流可信溯源服务技术系列规范的一部分，完善标准体系化建设。

本文件作为冷链可信溯源服务技术系列规范的一部分，旨在对冷链物流过程中涉及到的信息系统的通用安全技术要求进行约束，主要包括鉴权与安全防护要求、软件安全要求、数据安全要求、通信安全要求、个人隐私信息安全要求、系统审计安全要求六个技术安全要求。

冷链物流可信溯源服务技术要求　第3部分：信息系统安全

1　范围

本文件规定了冷链物流可信溯源技术服务的信息系统（如ERP、OMS、WMS、TMS等）在鉴权接入、软件系统、数据、通信及个人隐私方面的安全要求。

本文件适用于冷链物流技术服务提供商规范信息系统安全防护能力，也适用于冷链物流运营者、第三方评估机构对信息系统安全防护能力进行评估时参考。

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。

GB/T 18354-2006　物流术语

GB/T 21028-2007　信息安全技术 服务器安全技术要求

GB/T 22240-2008　信息系统

GB/T 28577-2012　冷链物流分类与基本要求

GB/T 28843-2012　食品冷链物流追溯管理要求

GB/T 35273-2020　信息安全技术 个人信息安全规范

GB/T 38155-2019　重要产品追溯 追溯术语

GB/T 38674-2020　信息安全技术 应用软件安全编程指南

GB/T 39786-2021　信息安全技术 信息系统密码应用基本要求

3　术语和定义

GB/T 18354-2006和GB/T 39786-2021界定的以及下列术语和定义适用于本文件。

3.1

冷链物流　cold chain logistics

以冷冻工艺为基础、制冷技术为手段，使冷链物品从生产、流通、销售到消费者的各个环节中始终处于规定的温度环境下以保证冷链物品质量，减少冷链物品损耗的物流活动。

[来源：GB/T 28577-2012，定义3.4]

3.2

追溯　traceability

通过记录和标识，追踪和溯源客体的历史、应用情况或所处位置的活动。

[来源：GB/T 38155-2019，定义2.2]

4　缩略语

下列缩略语适用于本文件。

ERP：企业资源计划系统（Enterprise Resource Planning）
OMS：订单管理系统（Order Management System）
WMS：仓库管理系统（Warehouse Management System）
TMS：运输管理系统（Transportation Management System）
API：应用程序接口（Application Programming Interface）

5 信息系统安全要求

5.1 鉴权与安全防护要求

5.1.1 身份认证与鉴权要求

信息系统中身份认证与鉴权应满足以下要求：

a) 应在用户登录系统之前进行鉴权，并在每次登录时就身份进行认证与鉴权；
b) 系统应具备远程控制请求的身份验证和接入认证机制，避免非法用户或应用控制系统，并对授权用户的远程会话进行加密保护；
c) 不同组织间通过 API 传输敏感数据时，应至少使用白名单（IP、域名等）方式进行控制， 同时应使用数字签名、开放标准认证（OAuth）等方式对调用的信息系统进行认证，确保对接口调用的鉴权；
d) 密钥、身份凭证等认证信息应具有时效性并限定作用域，认证信息超时或超出作用域后应重新分配。

5.1.2 系统防护要求

信息系统防护应满足以下要求：

a) 应采取安全措施，防范会话劫持、重放、中间人、拒绝服务等攻击。
b) 系统应该具备防火墙，能够抵抗常见的攻击手段，避免过滤规则被绕过。
c) 应在经过充分测试评估后，通过 OTA 更新、手动升级或其他方式进行安全漏洞修复。

5.2 软件安全要求

软件运行环境应满足 GB/T 21028-2007 服务器安全技术要求，同时软件研发应满足 GB/T 38674-2020 规定外，还应满足以下要求：

a) 对所有从客户端传入的数据不应信任，传入参数应使用白名单策略过滤可用字符/可能取值，对于可以明确定义范围的参数要校验参数有效性；
b) 不允许直接根据用户输入的参数拼接 sql 的情况出现，避免出现 SQL 注入；
c) 对上传文件的处理时，需要考虑对文件的扩展名进行白名单判断，对文件的内容进行判断，并将上传的文件按照一定规则改名并放到其它目录下保存；
d) 对于提供动态下载或读写删文件的功能，需要对文件路径、文件名都进行检查，不允许出现“../”、NULL 字符等文件系统特殊字符；
e) 避免出现执行系统命令的情况。如果出现，且需要将用户输入的参数带入命令行作为参数执行，需要将用户参数中的命令行特殊符号，如单引号、双引号、管道符、重定向符号、&符号、括号等符号进行过滤。防止被利用攻击服务器；
f) 程序错误信息对外界屏蔽：对程序的错误和异常进行专门的日志记录，避免直接输出给用户。特别是与文件或数据库相关的操作；
g) 项目使用的框架应以官方推荐的最新稳定版本为基础。

5.3 数据安全要求

冷链物流信息系统所涉及的数据处理，包括数据的收集、存储、使用、加工、传输、提供、公开等，数据安全是指通过采取必要措施，确保数据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。冷链物流信息系统数据安全除应遵守GB/T 35273—2020中规定的要求外，同时还应满足以下要求：

a) 数据访问
- 应以最小化原则设置敏感数据访问权限，仅限特定用户/应用访问；
- 应使用密钥、身份凭证等鉴权认证机制保护采集到数据，严格校验访问者是否具有数据的访问权限，禁止非授权访问、非法使用，防止出现数据泄露。

b) 数据存储
- 冷链物流追溯信息全程应保持信息记录的连续性和完整性,具备对数据完整性进行检测的能力，并提供相应的恢复控制措施；

注：冷链物流追溯信息应至少包含附录 A 中定义的信息，食品、酒类、医药产品、化学品等特定物品可参照附录 B。

- 数据宜至少保存两年，法律法规另有规定的除外。

c) 数据修改
- 冷链物流追溯信息应从技术上保证不可篡改，确需修改的，应记录详细操作内容和数据更改；
- 冷链物流系统中涉及到的敏感数据操作要有操作记录,操作日志保存时间不得短于记录保留时间，确保可追溯。

5.4 通信安全要求

冷链物流信息系统通信安全应满足以下要求：

a) 通过互联网传输信息时，应选择支持加密传输等安全扩展功能的通信协议，并且启用协议的安全功能。如果使用的通信方式存在国家标准，宜与国家标准保持一致。

b) 对于常见的带有 TLS 的通信协议(如 https),TLS 协议应使用 1.2 及以上版本，并对公钥、证书等进行校验；若使用 TLCP 协议，则应使用 1.1 及以上版本，应避免使用已知存在漏洞的协议。对于无法使用 TLS 的场景，应采用具有同等级安全性的通信协议、密码算法，并做好密钥保护工作。

5.5 个人隐私信息安全要求

除应遵守GB/T 35273—2020中规定的要求外，同时还应满足以下要求：

a) 应遵循最小化原则设置个人隐私信息的共享权限。在必须要进行个人隐私数据共享情况下，应对个人身份信息、电话号码、地址等敏感信息采用相应的安全措施，不限于加密、脱敏、去标识化等。

b) 寄送实名、运输司机实名等身份识别场景，如涉及收集个人信息生物识别信息，应采用符合一定安全强度标准的信息摘要算法存储摘要信息，并与个人身份信息分开存储。

5.6 系统审计安全要求

冷链物流信息系统审计安全应满足以下要求：

a) 冷链物流信息系统服务运营者应对数据使用保留日志记录，日志中包含敏感信息时，应对敏感数据进行脱敏处理。

b) 冷链物流信息系统中，对于敏感数据的异常操作（大量的删除、修改、导出、查询等）应进行

监控审计，及时发现异常操作。

附 录 A
（规范性）
冷链物流追溯信息内容

表A.1给出了冷链物流追溯应包含的信息内容。

表A.1 冷链物流追溯信息内容

信息类型	信息内容
商品信息	名称、通用名、批次、批号、有效期、生产厂家、品牌、数量、单位、重量、体积、数量、价值等
温、湿度信息	环境温、湿度记录、产品温湿度记录(采集时间和温湿度)、运输载体或仓库名称、运输时间或仓储时间
运输信息	收、发货方基本信息（包括名称、地址、联系人及联系方式等）、承运商信息（包括承运商名称、法人信息、车牌号、司机、身份证、联系方式）、押运人员信息（姓名、身份证号）、收发货时间、车辆在途信息等
仓储信息	仓库名称及地址、货位号、托盘/周转箱编码、收发货时间、操作人员等
其他信息	外包装状况、产品质量信息、调换信息、退回/销毁信息等

附 录 B
（规范性）
特定物品冷链物流追溯信息内容

食品物流追溯信息应包括GB/T 37029-2018中6.2的内容。
食品冷链物流追溯应符合GB/T 28843-2012的规定。
酒类商品物流追溯应包括产地、度数等信息，应符合 WB/T 1053-2015 的规定。
医药产品追溯应包括生产批号、保质期等信息。
化学品追溯应包括存储及运输环境信息、容器设备等清洗信息等信息。
其他商品的物流追溯信息应按照相关法律法规、标准及行业惯例记录。

电信终端产业协会团体标准

冷链物流可信溯源服务技术要求　第 3 部分：信息系统安全

T/TAF 101.3-2021

*

电信终端产业协会印发
地址：北京市西城区新街口外大街 28 号
电话：010-82052809
电子版发行网址：www.taf.org.cn