ICS 33.050
CCS M 30

团　体　标　准

T/TAF 101.2-2021

冷链物流可信溯源服务技术要求　第2部分：设备安全

Trusted and traceable service technical requirement for the cold chain logistics—Part 2: Device 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

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。

本文件主要起草人：林道正、焦龙龙、王靖琦、国炜、徐晓娜、李汝鑫、陈飞飞、刘献伦、刘为华、康亮、杨国东、黄德俊、杨超。

引　言

冷链物流涉及众多类型的设备，例如储存（冷库、冷藏箱、保温箱、低温冰柜或其他低温储存箱体等）、运输（如冷藏车、保温车、冷藏集装箱、冷藏船、冷藏火车/专列、附带冷藏箱/保温箱的运输设备等）、装卸以及温度记录仪或其他专门的设备，而伴随着物联网技术的不断发展，冷链物流中也存在众多独立或附属的物联网智能终端，通过设备内的操作系统、应用以及大量的第三方库，以提供冷链物流过程中相应的数据采集、传输等能力。

冷链物流中各类设备在设计、性能等方面上已有相关的标准规范（如 GB/T 28577），与此同时，随着物联网智能终端的广泛应用，此类设备在使用过程中的安全问题也引起越来越多的关注。然而，现有的一些物联网智能终端中硬件设计可能未考虑安全性，软件系统也通常是由不同的人员开发完成，因此设备的安全性往往并不能够得到保障。另一方面，随着各类产品迭代加速以及业务的拓展，物联网智能终端承担的功能越来越丰富，设备的版本也越来越多，而在不断的迭代过程中，容易产生典型的安全问题，这为冷链物流过程中对设备的管理、数据的溯源都会带来或多或少的障碍。

本文件主要针对冷链物流中物联网智能终端的硬件、软件、数据、通信等方面，制定通用的设备安全技术要求。从而实现各个物联网智能终端在其生命周期内具备必要的安全性，防止其成为冷链物流过程中的薄弱环节，提高冷链物流过程的安全性。

冷链物流可信溯源服务技术要求　第2部分：设备安全

1　范围

本文件针对冷链物流中物联网智能终端，规定了其需要满足的通用设备安全技术要求，包括硬件安全要求、软件安全要求、通信安全要求、升级安全要求、数据安全要求、鉴权与安全防护。

本文适用于参与冷链物流全流程各环节的物联网智能终端设备，个别条款不适用于特殊设备，其他类似设备也可参考使用。

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 35273-2020　信息安全技术 个人信息安全规范

GB/T 38626-2020　信息安全技术 智能联网设备口令保护指南

T/TAF 023-2018　移动智能终端应用软件安全与质量要求

T/TAF 079-2021　移动智能终端及应用软件生物特征识别安全规范

T/TAF 101.1-2021　冷链物流可信溯源服务技术要求 第1部分：总则

3　术语和定义

T/TAF 101.1-2021界定的以及下列术语和定义适用于本文件。

3.1

物联网　Internet of Things

物联网（简称IoT），通过感知设备，按照约定协议，连接物、人、系统和信息资源，实现对物理和虚拟世界的信息进行处理并做出反应的智能服务系统。

[来源：GB/T 33745-2017，　2.1.1]

3.2

单功能设备　single function device

单功能设备是基于轻量级嵌入式系统（如RTOS）或无操作系统，无法安装应用软件，功能较为单一的物联网智能终端设备，例如条码扫描设备、智能温感识别设备等。

3.3

多功能设备　multi-function device

多功能设备是基于复杂操作系统（如安卓），能够提供API接口，并能够安装、加载、运行应用软件，为用户提供多种功能的物联网智能终端设备，例如手持安卓终端。

4　缩略语

下列缩略语适用于本文件。

API：应用程序编程接口（Application Programming Interface）

CNNVD：中国国家信息安全漏洞库（China National Vulnerability Database of Information Security）

CNVD：国家信息安全漏洞共享平台（China National Vulnerability Database）

RTOS：实时操作系统（Real Time Operating System）

TLS：传输层安全（Transport Layer Security）

TLCP：传输层密码协议（Transport Layer Cryptography Protocol）

5 安全架构

冷链物流中使用的物联网智能终端,根据其实现方式以及对外提供的功能，可以划分为两种类型：

a） 基于轻量级嵌入式系统或无操作系统，无法安装应用软件，功能较为单一的单功能设备；

b） 基于复杂操作系统，能够安装、加载、运行应用软件，为用户提供多种功能的多功能设备。

两类设备均由硬件+软件的方式构成，其安全属性具有共性，整体的安全架构基本相同，如图1所示，主要包含6个部分：最底层是硬件安全，其上为软件安全、升级安全、通信安全，数据安全、鉴权与安全防护则同时涉及这4个层面。

图 1 物联网智能终端设备安全框架

其中：

a） 硬件安全：保证设备内处理器、存储和接口的安全，在芯片级对设备进行保护，防止芯片内的程序、数据被非法访问、篡改。

b） 软件安全：保障固件、操作系统以及应用安全，对系统、应用进行安全配置，保护设备业务、权限。

c） 通信安全：保障设备数据传输过程的安全性。

d） 升级安全：在升级更新时加强保护，防止因升级过程降低安全性。

e） 数据安全：保障数据在采集、传输、存储、处理过程中的安全性。

f） 鉴权与安全防护：通过恰当的安全配置，防范越权行为，遏制潜在的攻击。

物联网智能终端设备的安全要求分为两部分，第6章规定了两类设备均需满足的通用安全技术要求，第7章规定了多功能设备在通用要求基础上仍需满足的扩展安全技术要求。

6 通用安全技术要求

6.1 硬件安全要求

6.1.1 硬件接口安全

设备的硬件接口应符合以下要求。

a） 应遵循最小化原则，保证在出厂后显式调试接口等非必需的物理接口已被禁用。

b） 应去除隐式调试接口或去除隐式接口的部分器件、添加接口验证。

c） 当设备具备控制台接口时，必须为接口添加安全访问控制措施，防止未授权访问。

注：可使用口令或其他方式进行访问控制。

6.1.2 物理安全

宜去除设备电路板中芯片、接口、管脚的标记。

6.2 软件安全要求

6.2.1 系统安全要求

6.2.1.1 安全启动

宜在固件启动时，提供安全启动机制，确保只加载执行可信的固件。

6.2.1.2 权限配置

系统中的权限配置应符合以下要求。

a） 应开启地址随机化、堆栈不可执行等安全配置，应为关键区域设置正确的权限。

b） 应对关键系统API提供访问控制机制，防止非授权的API调用。

c） 不应将用户名、口令等敏感信息明文存储在固件中。

6.2.1.3 服务配置

系统中的服务配置应符合以下要求。

a） 应遵循最小化原则，移除非必需的服务，例如远程调试；对必须保留的服务，必须添加安全访问控制措施，防止未授权用户使用服务，并在使用完成后立即关闭。

b） 对外开放的服务，不应以最高权限（如root权限）运行。

c） 不应存在后门、隐藏接口/服务。

d） 应具备修改服务默认配置的功能。

e） 对于能够远程访问的服务，所有操作行为均应通过认证，并通过日志记录操作过程。

6.2.1.4 漏洞管理

系统中不应存在CNVD、CNNVD等权威漏洞平台，公开发布6个月以上的高危及以上安全漏洞。

6.2.2 第三方组件安全要求

系统中使用的第三方组件应符合以下要求。

a） 应使用主流、安全的第三方组件，从可靠的来源获取第三方组件，并在保证稳定的情况下尽可能采用最新版本。

b） 应及时更新第三方组件的版本，应特别关注包含安全问题修复的版本，并及时将第三方组件更新至无已知安全问题的版本。

c） 不应使用存在已知重大安全问题的第三方组件版本，不应使用不再正常维护更新、无法及时修复安全问题的第三方组件。

6.2.3 日志安全要求

日志功能应符合以下要求。

a) 设备本身或其关联设备应具备记录用户操作，异常关机、重启、数据损坏等异常状态，以及其他关键事件的功能，记录的内容至少包括时间、对象、描述、结果以及其他与安全审计相关的信息。
b) 应采取必要的措施保护日志记录过程，防止出现非预期的中断。
c) 应在存储时保证日志记录完整性。
d) 不应在日志中记录敏感信息。
e) 应具备对空间不足、存储错误等异常情况的处理措施。
f) 应支持日志上传至云端进行管理，并保证日志传输时的机密性、完整性，云端日志记录的存储时间应满足安全溯源要求（至少6个月）。
g) 日志记录应进行访问控制，保护日志不被非法访问、篡改，并应仅允许管理员执行日志的删除操作。

6.3 通信安全要求

设备的通信过程应符合以下要求。

a) 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。
b) 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。
c) 应安全实现通信协议，预防因编程语言的固有缺陷而可能造成的安全问题。
d) 当传输敏感数据时，应使用安全的通信协议加密传输，宜使用TLCP1.1、TLS1.2或更高的版本，并避免明文数据、加密数据混合传输。
e) 应具备加密机制，保证通信过程中敏感数据的机密性。
f) 应具备完整性校验机制，保证通信过程中数据的完整性。
g) 加密算法宜使用ECC、SM4、AES 128或更高强度的算法，并应做好密钥保护工作；使用AES算法时应选择安全的工作模式，不应使用ECB、CBC等不安全的模式。
h) 完整性校验算法宜使用SM3、SHA-256、SHA-384或更高强度的算法。
i) 应具备异常数据处理能力，防止出现非预期的异常情况，并避免错误提示信息被攻击者利用。
j) 宜在通信前进行双向身份认证,并采取必要的保护措施，防止相关身份认证信息被截获、仿冒、重用。

6.4 升级安全要求

设备应支持升级更新，并符合以下要求。

a) 除用户或管理者主动将升级过程设置为不提示的自动升级外，升级之前应有提示，不应强制更新。
b) 通过网络传输升级包时应采用安全的通信协议，宜使用TLCP1.1、TLS1.2或更高的版本。
c) 传输升级包时宜采用双向身份认证。
d) 宜对升级包进行加密，宜使用SM4、AES 128或更高强度的算法，使用AES算法时选择安全的工作模式，不应使用ECB、CBC等不安全的模式。
e) 升级时，应对升级包的完整性进行校验，防止升级包被篡改。
f) 升级时，应对升级包的版本进行校验，防止降级更新。
g) 系统升级失败时，应保持原系统的可用性，并且安全属性与升级前一致。

6.5 数据安全要求

设备中数据的处理应符合以下要求。

a) 个人信息的处理应遵守GB/T 35273-2020（所有部分）中规定的要求。
b) 应采取必要的保护措施，保证数据在传输、存储时的机密性、完整性，且相关的密钥不应硬编码在代码中。
c) 应避免存储用户个人的敏感数据，必须存储时应加密存储，且加密算法应符合国家法律法规的规定，并实现访问控制，防止非授权的访问、篡改。
d) 应避免将敏感数据输出至日志系统。
e) 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。
f) 应使用密钥、身份凭证等鉴权认证机制保护数据，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。
g) 应在敏感数据的存储空间被释放或重新分配前进行完全清除，防止可能的数据泄露。
h) 应采取必要的措施，保证数据被销毁时，能够清除所有副本，并利用技术手段避免原始数据被恢复。

6.6 鉴权与安全防护

设备中的鉴权与安全防护措施应符合以下要求。

a) 存在默认账户时，应支持修改默认账户的口令。
b) 应删除无用的账户和访问控制规则。
c) 应以最小化原则进行权限配置。
d) 对于访问权限有要求的接口、数据等，应具备访问控制机制。
e) 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。
f) 当使用口令机制时，应遵守GB/T 38626-2020中第7章规定的要求。
g) 不应存在后门、隐藏接口、恶意代码。

7 多功能设备增强安全技术要求

7.1 硬件安全要求

7.1.1 芯片安全

设备中使用的芯片应符合以下要求。

a) 设备应具备不可改写的安全存储区域，用于存储校验密钥等信息。
b) 设备应具备必要的固件保护措施，包括但不限于加密、签名、写保护等，防范固件被提取、篡改。
c) 设备宜具备物理保护能力，防止攻击者通过去除封装等物理接触方式，获取芯片内部存储的数据。
d) 若设备需要对生物特征识别信息等敏感数据进行操作，应具备安全芯片或可信执行环境。

7.1.2 物理安全

设备宜具备对自身状态的检测能力，在出现暴力移除、拆卸、替换等情况时，提供必要的告警机制。

7.2 软件安全要求

7.2.1 系统安全要求

7.2.1.1 安全启动

应在固件启动时，提供安全启动机制，确保只加载执行可信的固件，并符合以下要求。

a) 应从不可篡改的区域开始执行安全启动，并在启动过程中校验密钥的完整性、真实性。
b) 应在安全启动过程中校验镜像的完整性、真实性；当存在多级启动时，每个镜像启动前均应进行校验。
c) 安全启动过程中应校验镜像的版本，不应启动比设备存储的版本号低的镜像；镜像的版本号信息应储存在不可直接访问、具备防篡改能力的区域。
d) 安全启动过程中应禁用调试。
e) 安全启动过程中任意步骤校验不通过或出现其他失败情况，应退出启动过程，并清除RAM中的数据。

7.2.1.2 权限配置

系统中的权限配置应符合以下要求。

a) 应遵循最小化原则，为不同的用户、应用分配权限，禁止越权操作。
b) 应开启SELinux或其他强制访问控制策略等安全配置。
c) 应采取适当的访问控制措施对不同用户、应用的数据进行隔离，防止非授权访问。
d) 应禁止root用户非授权登录，默认禁止任何进程或应用获取系统的超级用户权限，防范可能的提权攻击。
e) 不应存在隐藏账号。
f) 应提供登录失败处理，限制非法登录次数。

7.2.2 应用安全要求

应用安全应符合T/TAF 023-2018中第4章规定的要求，并符合以下要求。

a) 应开启地址随机化、堆栈不可执行等保护措施，并去除符号表信息。
b) 不应存在后门隐藏接口。
c) 不应将用户名、口令等敏感信息明文存储在应用中，或硬编码在代码中。
d) 有登录功能的情况下，应提供限制非法登录次数或其他登录失败处理。
e) 支持多用户的情况下，应采取访问控制措施对不同用户的数据进行隔离，防止越权访问。
f) 应禁止安装官方渠道以外的应用。
g) 宜使用白名单机制管理设备上的应用，禁止非白名单应用安装、运行。
h) 应用宜对自身的完整性、机密性、可用性等进行验证。
i) 宜使用加固技术对应用进行保护。

7.3 通信安全要求

通信过程中宜采取安全措施，防范ARP欺骗、DNS劫持、伪Wi-Fi热点、伪基站、会话劫持、重放、拒绝服务等攻击。

7.4 升级安全要求

设备的升级更新应符合以下要求。

a) 应用升级失败时，应保持原应用的可用性，并且安全属性与升级前一致。
b) 宜定期更新设备中存储的工厂包。
c) 宜支持热修复，用于在出现安全问题时，快速执行修复操作。

7.5 数据安全要求

设备中数据的处理应符合以下要求。

a) 生物特征识别信息的存储、使用应符合T/TAF 079-2021中第6、7章规定的要求。

b) 对生物特征识别信息等敏感数据进行操作时，应采用安全芯片或可信执行环境进行相应的处理，以保证数据安全性。

7.6 鉴权与安全防护

设备中的鉴权与安全防护措施宜符合以下要求。

a) 宜采用校验技术对关键代码、数据进行完整性保护。

b) 宜能够检测到对重要位置的攻击行为，如网络攻击、异常流量、会话劫持，并且在检测到攻击行为时采取日志记录、安全告警、攻击遏制等措施。

参 考 文 献

[1] GB/T 38636 信息安全技术 传输层密码协议（TLCP）
[2] YD/T 2407-2013 移动智能终端安全能力技术要求

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 2 部分：设备安全

T/TAF 101.2-2021

*

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