ICS **
CCS **

团 体 标 准

T/ITS XXXX-XXXX

智慧云收费终端信息安全技术要求

Information Security Technical Requirements for Intelligent Cloud-based Toll Collection Terminals

20**-**-**发布 2020-**-**实施

中国智能交通产业联盟 发布

目　　次

前　言

本文件按照GB/T1.1—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。

本文件由中国智能交通产业联盟提出并归口。

本文件起草单位：中路高科交通科技集团有限公司、甘肃新陆港科技有限公司、北京邮电大学、北京航空航天大学、哈尔滨工业大学（深圳）、江西省交通监控指挥中心、北京市首都公路发展集团有限公司、特微乐行（广州）技术有限公司、北京速通科技有限公司、浙江数智交院科技股份有限公司、深圳市金溢科技股份有限公司、中信科智联科技有限公司、联通智网科技股份有限公司。

本文件主要起草人：

智慧云收费终端信息安全技术要求

1 范围

本文件规定了高速公路智慧云收费终端信息安全管理体系要求、信息安全技术要求，描述了相应的测试与验证方法。

本文件适用于高速公路智慧云收费终端产品的设计、开发与检测，为高速公路管理部门、运营机构等实施高速公路智慧云收费终端的安全防护提供技术参考。

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 25069-2022 信息安全技术 术语

GB/T 29240-2024 网络安全技术 终端计算机通用安全技术规范

GB/T 46141-2025 智慧城市基础设施 智慧交通数字化支付应用指南

JT/T 1522-2024 交通运输数据安全分级和保护要求

3 术语、定义和缩略语

3.1 术语和定义

下列术语和定义适用于本文件。

3.1.1

智慧云收费终端 Intelligent Smart Cloud Payment Terminals

智慧云收费终端部署在收费站车道侧，主要包括岛头智能节点、岛尾智能节点、车道智能终端、ETC特情处置终端、智慧收费亭、自动关道机、手持终端、称重设备等。

3.1.2

ETC特情处置终端 Etc Exception Handling Terminal

部署于收费公路ETC车道现场，用于辅助处理电子不停车收费过程中因交易失败、信息异常或业务逻辑拒绝等原因导致无法正常通行的车辆，支持用户自助操作与远程协同处置，并具备身份鉴权、安全通信、交易处理及日志审计能力的专用智能外设终端。

3.1.3

收费类终端 Toll Transaction Terminal

直接执行电子收费核心业务功能的智慧云收费终端，具备交易处理、特情处置、人机交互等能力，用于保障收费过程的高效性、准确性与安全性，如ETC特情处置终端、车道智能终端、手持收费终端、智慧收费亭等。

3.1.4

辅助收费类终端 Auxiliary Toll Support Terminal

不直接参与收费交易，但用于实时感知车道运行状态及车辆通行信息，为收费业务提供关键数据支撑的智慧云收费终端，如岛头智能节点、岛尾智能节点等。

3.1.5

重要数据 Critical Data

指与收费业务相关的，一旦泄露可能直接影响运营方经济利益或公共利益的非个人信息，如交易流水、费率策略、终端配置信息等。

3.1.6

终端操作系统 Terminal Operating System

终端上运行的操作系统，如嵌入式Linux、Android等。

3.1.7

访问控制 Access Control

确保只有授权用户才能访问授权资源的技术手段。

3.1.8

安全审计 Security Auditing

对系统安全相关活动进行记录、分析和检查，以发现安全漏洞和行为异常。

3.2 缩略语

下列缩略语适用于本文件。

JTAG：联合测试工作组（Joint Test Action Group）

UART：通用异步收发器（Universal Asynchronous Receiver/Transmitter）

USB：通用串行总线（Universal Serial Bus）

SDL：安全开发生命周期（Security Development Lifecycle）

OTA：空中下载技术（Over-The-Air Technology）

4 智慧云收费终端总体构成

智慧云收费终端总体构成，见图1所示。

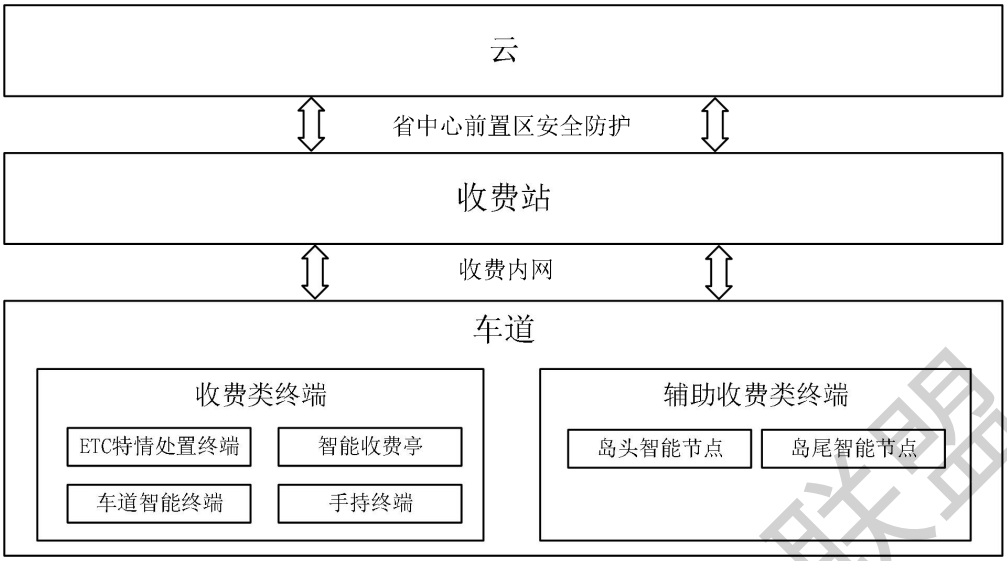

图 1 智慧云收费终端总体构成图

根据各业务模块功能特点，可将智慧云收费终端划分为两大类：收费类终端和辅助收费类终端。

收费类终端，承担交易处理、特情处置、人机交互等核心收费功能的相关设备，主要包括：ETC特情处置终端、车道智能终端、手持终端、智慧收费亭等。该类终端直接面向收费业务执行，对交易数据的完整性、保密性及系统业务连续性方面具有较高要求，是保障收费过程高效、准确、安全的关键环节

辅助收费类终端，负责对车道运行状态及车辆通行信息进行实时感知与采集，为收费业务提供关键数据支撑的相关设备，主要包括：岛头智能节点、岛尾智能节点等。该类终端对数据采集的准确性、实时性以及设备运行的稳定性具有较高要求，通过精准的车辆检测与通行信息采集，有效保障收费交易触发的及时性与准确性，是实现车道无人化、智能化管控的重要基础支撑。

5 智慧云收费终端信息安全管理体系要求

5.1 全生命周期管理要求

智慧云收费终端硬件、软件、网络等核心部件的生产方、建设方、运营方、管理方应具备智慧云收费终端全生命周期的信息安全管理体系。

注：智慧云收费终端全生命周期包括终端软硬件的开发阶段、生产阶段及后生产阶段。

5.2 安全管理体系内容

智慧云收费终端信息安全管理体系应包括以下内容：

a) 建立终端信息安全测试、网络准入、配置变更、漏洞修复、退役销毁等全环节的安全管理过程，包括：
   1) 建立用于智慧云收费终端软硬件信息安全测试的过程；
   2) 建立用于智慧云收费终端入网身份认证及健康检查的过程，并确保终端硬件、软件及网络风险评估保持正常、合法状态；
   3) 建立用于智慧云收费终端软件及网络配置变更审核的过程；

4) 建立识别、评估、分类、处置终端硬件、软件及网络信息安全风险及核实已识别风险得到处置的过程，并确保终端硬件、软件及网络风险评估保持最新状态；
5) 建立用于智慧云收费终端退役销毁安全管理的过程。

b) 建立针对智慧云收费终端的网络攻击、网络威胁和漏洞的监测、响应及漏洞上报过程，要求如下：
1) 包含漏洞管理机制，明确漏洞收集、分析、报告、处置、发布、上报等活动环节；
2) 建立针对网络攻击提供相关数据并进行分析的过程，如通过终端状态和运行日志等数据分析和检测网络攻击、威胁和漏洞；
3) 建立确保已识别的网络攻击、网络威胁和漏洞得到响应，且在时限内得到处置的过程；
4) 建立评估所实施的信息安全措施在发现新的网络攻击、网络威胁和漏洞的情况下是否仍然有效的过程；

c) 建立智慧云收费终端软硬件管理企业与合同供应商、服务提供商、道路交通物联网终端制造商子组织之间道路交通物联网终端信息安全依赖关系的过程，要求如下：
1) 建立智慧云收费终端安全风险分级管控策略，并确保所实施的信息安全措施在终端面临外部攻击、内部误操作、数据泄漏等安全风险时仍然有效；
2) 建立明确终端供应商的安全责任划分的过程，如要求供应商提供硬件安全芯片、固件签名验证等能力。

6 信息安全技术要求

6.1 硬件安全技术要求

智慧云收费终端硬件安全技术要求应包括以下内容：

a) 智慧云收费终端应具备防拆防篡改的物理安全措施（如防拆开关、封签、加固外壳等），一旦检测到非法开启或破坏，须自动清除敏感数据并生成不可篡改的安全日志；
b) 智慧收费亭应具备受控物理门禁机制仅允许授权人员进入，门禁系统需支持身份认证如 IC 卡、生物识别或双因素认证等并记录所有出入事件日志，日志应包含时间、人员标识和操作类型等信息且具备防篡改存储能力，当检测到非法闯入或门禁异常时需触发安全告警并可联动亭内终端设备执行敏感数据保护措施；
c) 智慧云收费终端的调试和维护接口（如 JTAG、UART、USB 等）应在出厂时默认关闭，如需启用应通过授权认证并产生审计记录；
d) 收费类终端应具备符合国家密码管理要求的安全芯片，实现密钥安全存储、身份认证、交易签名及敏感数据保护等核心安全功能。

6.2 软件安全技术要求

智慧云收费终端软件安全技术要求应包括以下内容：

a) 软件开发应遵循安全开发生命周期（SDL），包括威胁建模、安全编码、代码审计与漏洞测试，确保应用不存在已知高危漏洞；
b) 收费类终端上的操作系统、中间件、应用软件及固件应定期进行安全评估，确保不存在 CNVD、CNNVD 或 NVD 等平台已公开且未修复的高危及以上漏洞，对已识别漏洞须在规定时限内完成修复或采取有效缓解措施；
c) 收费类终端操作系统及应用软件应支持完整性校验，运行过程中关键进程和库文件不得被篡改，一旦发现异常应触发告警；

d) 收费类终端应具备安全的远程软件升级能力，升级包需由可信签发方进行数字签名并在安装前验证其有效性与完整性，升级数据的传输过程应采用国密加密机制进行保护，升级过程须具备原子性以实现失败后自动回滚至升级前稳定版本，并生成不可篡改的安全审计日志；
e) 终端设备上的软件模块应遵循最小权限原则，不同功能模块之间应隔离运行，避免单点突破引发系统级风险；
f) 终端设备中的关键密码算法实现及核心应用代码应采取代码混淆、存储加密、运行时完整性保护和反调试等安全防护措施，防止被逆向分析、篡改或非法复制；相关保护机制应确保在未授权环境下无法提取或还原敏感逻辑与密钥信息；
g) 智慧云收费终端宜对自身设备状态进行监测，如在线/离线状态等，并支持向云平台报送的能力。

6.3 通信安全技术要求

智慧云收费终端通信安全技术要求应包括以下内容：
a) 智慧云收费终端应使用自建有线专网或运营商专线作为网络接入通道；
b) 智慧云终端应具有可用于云智慧收费中网络通信识别的唯一标识，并且该标识应具备防篡改保护能力；
c) 智慧云终端应具备网络访问控制能力，应能根据 IP 地址设置网络通信黑/白名单；
d) 辅助收费类终端宜采用数字证书认证技术及国家密码主管部门认可的密码算法实现远程接入时的身份认证；
e) 收费类终端应采用数字证书认证技术及国家密码主管部门认可的密码算法实现远程接入时的身份认证；
f) 辅助收费类终端宜采用国家密码主管部门认可的密码算法实现机密性和完整性保护；
g) 收费类终端应采用国家密码主管部门认可的密码算法实现机密性和完整性保护；
h) 收费类终端应具备抗重放与抗中间人攻击能力，对关键交易信息和控制指令应使用随机数、会话密钥等技术保证唯一性与实时性；
i) 智慧云终端宜具备网络攻击检测功能，当检测到攻击行为时，应记录攻击源 IP、攻击类型、攻击时间，在发生严重入侵事件时应提供报警。

6.4 数据安全技术要求

智慧云收费终端数据安全技术要求应包括以下内容：
a) 智慧云收费终端数据分级应符合 JT/T 1522-2024 中 4.5 的规定，核心数据、重要数据、一般数据按照合 JT/T 1522-2024 中 5.3 的分级保护要求进行安全防护；
b) 智慧云收费终端应采取安全访问技术、只读技术等安全防御机制保护存储在终端内的核心业务配置文件，防止其被非授权删除和修改；
c) 智慧云收费终端应采取安全防御机制保护存储在终端内的安全日志，防止其被修改和非授权删除；
d) 辅助收费类终端应采取安全访问技术、加密技术或其他安全技术保护车辆识别过程中的敏感个人信息，防止其被非授权访问和获取；
e) 收费类终端应采取安全访问技术、加密技术或其他安全技术保护收费过程中的敏感个人信息，防止其被非授权访问和获取；
f) 智慧云收费终端不应直接向境外传输数据。

7 测试与验证方法

7.1 硬件安全测试

7.1.1 安全启动测试

测试方法：

a) 使用工具修改操作系统或关键应用软件的镜像文件；
b) 尝试启动被篡改镜像的终端设备；
c) 观察终端启动过程中的验证行为。

预期结果：终端应检测到镜像完整性被破坏，拒绝启动并记录安全事件。

7.1.2 安全存储测试

测试方法：

a) 通过物理方式提取存储芯片；
b) 使用专业设备读取存储内容；
c) 分析获取的数据内容。

预期结果：敏感数据应以加密形式存储，无法直接读取明文信息。

7.1.3 物理防护测试

测试方法：

a) 尝试拆卸终端外壳；
b) 拔插关键接口；
c) 监测防拆机制的触发情况。

预期结果：拆卸行为应触发数据清除功能，并生成安全告警日志。

7.2 软件安全测试

7.2.1 OTA 升级安全测试

测试方法：

a) 伪造数字签名生成升级包；
b) 模拟中间人攻击篡改传输中的升级包；
c) 故意中断升级过程。

预期结果：终端应拒绝非法签名包，检测传输篡改，升级失败时自动回滚。

7.2.2 代码保护测试

测试方法：

a) 使用反编译工具分析核心代码；
b) 尝试进行动态调试；
c) 分析代码的可读性和结构。

预期结果：核心代码应经过有效混淆和加密，无法进行逆向分析。

7.2.3 安全审计测试

测试方法：

a) 执行各类操作（登录、参数修改等）；
b) 检查审计日志记录完整性；
c) 尝试进行日志溯源分析。

预期结果：日志应完整记录操作行为，支持多维度查询和分析。

7.3 通信安全测试

7.3.1 内部通信测试

测试方法：

a) 监听终端与车道控制器、云平台间通信；
b) 尝试中间人攻击；
c) 分析通信协议和加密强度。

预期结果：通信应建立加密通道，抵抗中间人攻击。

7.3.2 外部通信测试

测试方法：

a) 模拟非法设备尝试连接；
b) 伪造设备身份信息；
c) 分析身份验证机制。

预期结果：应拒绝非法设备连接，验证设备身份合法性。

7.3.3 网络隔离测试

测试方法：

a) 从办公网络尝试访问终端网络；
b) 从互联网尝试访问终端网络；
c) 测试网络连通性。

预期结果：网络间应实现物理隔离，无法跨网访问。

7.4 数据保护测试

7.4.1 数据脱敏测试

测试方法：

a) 查询系统各类界面显示；
b) 检查数据库存储内容；
c) 分析日志记录信息。

预期结果：敏感信息展示时应进行脱敏处理。

7.4.2 数据加密测试

测试方法：

a) 抓取网络传输数据；
b) 分析存储数据格式；
c) 验证加密算法符合性。

预期结果：数据传输和存储均应采用国密算法加密。

7.4.3 数据销毁测试

测试方法：

a) 执行数据销毁操作；
b) 使用数据恢复工具尝试恢复；

c） 分析存储介质底层数据。

预期结果：数据应被彻底清除且不可恢复。

7.5 测试报告要求

测试完成后应提供：

a） 详细的测试用例执行记录；

b） 发现的安全问题及风险等级；

c） 整改建议和验证结果；

d） 最终符合性结论。

T/ITS XXXX-XXXX

中国智能交通产业联盟
标准

智慧云收费终端信息安全技术要求

T/ITS XXXX-XXXX

北京市海淀区西土城路 8 号（100088）
中国智能交通产业联盟印刷
网址：http://www.c-its.org.cn

20XX 年 XX 月第一版　20XX 年 XX 月第一次印刷