ICS 35.240.60
CCS L70

CIITA

团　　体　　标　　准

CIITA 204-2025

数字人民币 轨道交通自动售检票系统技术要求

e-CNY electronic payment—technical requirements for urban rail transit Automatic Fare Collection(AFC) system

2025-06-18 发布　　2025-07-01 实施

中国信息产业商会 发布

目　录

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。

本文件由中国信息产业商会交通数智化分会。

提出。

本文件由中国信息产业商会归口。

本文件起草单位：北京城建智控科技股份有限公司、南京熊猫信息产业有限公司、上海中软华腾软件系统有限公司、中铁第一勘察设计院集团有限公司、中铁二院工程集团有限责任公司、深圳市雄帝科技股份有限公司、青岛博宁福田智能交通科技发展有限公司、普天轨道交通技术上海有限公司、数金公共服务（青岛）有限公司、深圳市深圳通有限公司、上海信投智能科技股份有限公司、中交（天津）轨道交通运营管理有限公司。

本文件主要起草人：管宏、王欢、王峰、贾弛、于增佳、黄问遂、钱鸣、李宁、程亮、尤圣泉、吴婷、曹家玉、刘明丽、张成龙、白向宇、袁磊、张金明、韩宇峰、张振华、张利宽、生明华、熊辉、张东东、张兆俊、李海培、文璐、张活林、王伟、曹吉、刘明、徐亮、夏阳、刘霁锋、田博鹰、池晓彬、孙宝娣、杨向民、甄永峰、王健、陈小海、周世爽、杨承东、冯娟、李宇轩、吴华、杨波、张宝霞。

数字人民币 轨道交通自动售检票系统技术要求

1 范围

本文件规定了数字人民币应用对于城市轨道交通自动售检票系统的应用场景，提出了对线网中心系统、线路中央计算机系统及车站计算机系统、车站终端设备、通用读写器、软件系统以及系统安全的技术要求；提出了数字人民币“软钱包”和“硬钱包”的技术形态要求；提出了软钱包小额支付、在线授权硬钱包过闸和离线验证硬钱包过闸的应用场景下相对应的业务流程要求；提出了数字人民币在城市轨道交通售检票系统应用的运行环境、安全以及接口兼容性要求。

本文件适合于城市轨道交通及周边交通系统（如公交），在应用数字人民币作为支付方式或检票方式时，进行系统设计、建设、运营和改造时使用。

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。

ISO/IEC 14443 识别卡 非接触式集成电路卡 接近式卡（Identification cards - Contactless integrated circuit cards - Proximity cards）

JR/T 0025—2018 中国金融集成电路（IC）卡规范

GB/T 20907 城市轨道交通自动售检票系统技术条件

T/CAMET 11001.1 智慧城市轨道交通 信息技术架构及网络安全规范 第1部分：总体需求

T/CIITA 201.1—2021 城市轨道交通自动售检票系统第1部分：系统架构、业务规则及软件要求

T/CIITA 201.2—2021 城市轨道交通自动售检票系统第2部分：终端设备

T/CIITA 201.4—2021 城市轨道交通自动售检票系统第4部分：网络安全规范

T/CIITA 201.5—2021 城市轨道交通自动售检票系统第5部分：互联互通要求

3 术语和定义、缩略语

3.1 术语和定义

GB/T 20907、GB/T 50381、T/CIITA 201 界定的以及下列术语和定义适用于本文件。

3.1.1 自动售检票系统 automatic fare collection system

基于计算机、通信、网络、自动控制等技术，实现轨道交通售票、检票、计费、收费、统计、清分、管理等全过程的自动化系统。

[来源：GB/T 50381—2018 2.0.1]

3.1.2 线网中心系统 AFC network control central system

具备管辖范围内所有线路自动售检票系统的清分、互联网票务以及互联互通服务等功能的信息系统，且在管辖范围内具有唯一性。

3.1.3 线路中央计算机系统 line computer system

用于监控和管理城市轨道交通单线路自动售检票系统的计算机系统。。

[来源：GB/T 50381—2018 2.0.9]

3.1.4 金融 IC 卡 financial integrated circuit(s) card

符合 JR/T 0025—2018 要求的，由金融机构发行的集成电路（IC）卡。

3.1.5 车站计算机系统 station computer system

管理车站级的票务处理、设备运行、客流统计等的计算机系统。

[来源：GB/T 50381—2018 2.0.9]

3.1.6 车站终端设备 station level equipment

安装在城市轨道交通线路各车站，进行车票发售、进站检票、出站检票、充值、验票分析等交易处理的设备。

[来源：GB/T 50381—2018 2.0.2 有修改]

3.1.7 自动检票机 automatic gate machine

对车票进行自动检验和处理，放行或阻挡乘客出入付费区的设备。自动检票机分进站检票机、出站检票机和双向检票机三种类型。

[来源：GB/T 50381—2018 2.0.3 有修改]

3.1.8 半自动售票机 booking office machine

用于人工辅助发售、赋值有效车票，具备补票、退票、查询、更新等票务处理功能的设备。

[来源：GB/T 50381—2018 2.0.6]

3.1.9 自动售票机 automatic ticket vending machine

用于自助发售、赋值有效车票，具备自动处理支付和找零功能的设备。

[来源：GB/T 50381—2018 2.0.5]

3.1.10 多功能自助票务终端 multi function self-service ticketing terminal

具备票务自助处理、信息咨询服务、开具电子发票等功能，用于部分替代车站票务客服人员工作的设备。

3.1.11 便携式检验票机 portable card analyzer

工作人员进行检票和验票的手持设备。

3.1.12 数字人民币 electronic Chinese Yuan（e-CNY）

由中国人民银行发行的数字形式的法定货币，与实物人民币（纸钞、硬币）具有完全相同的法律效力和价值特征。

3.1.13 数字人民币运营机构（运营商）operating institution of e-CNY

负责数字人民币发行、运营和管理的银行或其他金融机构。

3.1.14 数字人民币商户 merchant of e-CNY

受理数字人民币业务的单位或个人。

3.1.15 数字人民币硬钱包 e-CNY hardware wallet

数字人民币硬钱包是指基于安全芯片等技术，依托 IC 卡、手机终端、SIM 卡、可穿戴设备、物联网设备等特定硬件载体为客户提供服务的数字人民币钱包。

3.1.16 数字人民币软钱包 e-CNY software wallet

是一种基于数字人民币的电子钱包应用，用户通过智能手机、平板电脑等终端设备下载官方指定的数字人民币 APP 或相关应用程序，实现数字人民币的存储、转账、支付及管理等功能。

3.1.17 访问令牌 Token

是在数字人民币应用过程中，具备验证用户身份、授权访问钱包和标识唯一交易等用途的一种数据标记凭证。

3.2 缩略语

下列缩略语适用于本文件。

ACC：自动售检票清分中心系统（AFC Central Clearing System）
AFC：自动售检票系统（Automatic Fare Collection System）
AGM：自动检票机（Automatic Gate Machine）
API：应用程序接口（Application Programming Interface）
BOM：半自动售票机（Booking Office Machine）
CRC：循环冗余校验（Cyclic Redundancy Check）
E/S：编码分拣机（Encoder/Sorter）
FTP：文件传输协议（File Transfer Protocol）
ITP：互联网票务平台（Internet Ticketing Platform）
ITVM：互联网售票机（Internet Ticket Vending Machine）
LC：线路计算机系统（Line Computer System）
MAC：消息认证码（Message Authentication Code）
NFC：近场无线通信（Near Field Communication）
OD：起止点（Origin & Destination）
PSAM：销售点终端安全存取模块（Purchase Secure Access Module）
RSA：RSA 加密算法（RSA algorithm）
SAM：安全存取模块（Secure Access Module）
SDK：软件开发工具包（Software Development Kit）
SE：安全单元（Secure Element）
SC：车站计算机系统（Station Computer System）
SFTP：安全文件传输协议（Secure FTP）
SLE：车站终端设备（Station Level Equipment）

SM2 ：椭圆曲线公钥密码算法（SM2 Elliptic Curve Public Key Cryptographic Algorithm）
SM3：密码杂凑算法（SM3 Cryptographic Hash Algorithm ）
SM4：分组密码加密算法（SM4 Block Cipher Algorithm）
STM：自助票务处理机（Self-service Ticketing Machine）
TAC：交易验证码（Transaction Authentication Code）
TVM：自动售票机（Ticket Vending Machine）
URL：统一资源定位器（Uniform Resource Locator）

4 应用场景

4.1 概述

依据钱包的不同存在方式，数字人民币的应用场景有：
——软钱包应用场景：通过移动支付 APP、软件开发工具包（SDK）、应用程序接口（API）等完成用户购票、补票支付乘车费用的操作。
——硬钱包应用场景：依托 IC 卡、手机终端、可穿戴设备等完成用户进出站检票并支付乘车费用的操作。

4.2 软钱包应用场景

4.2.1 线上支付

乘客线上购票时，选择支付方式为数字人民币，完成购票。
使用数字人民币线上支付前，与数字人民币软钱包签约，签约成功后方可使用数字人民币支付。签约可通过子钱包推送、轨道交通 App 端网页直连和 API 直连三种方式。

4.2.2 线下购票

乘客通过数字人民币软钱包“主扫”或“被扫”二维码，完成购票。

4.2.3 乘车码过闸

乘车码过闸时，选择数字人民币支付，其它流程与乘车码过闸一致。

4.3 硬钱包应用场景

对于已申请数字人民币硬钱包的用户，可使用数字人民币硬钱包作为乘车凭证检票进出站。钱包凭证的合法性验证分为在线验证和离线验证两种方式。对于行程信息不可回写的钱包应采用在线验证方式；对于行程信息可回写的钱包应采用离线验证方式。

4.3.1 在线验证过闸

检票机读取数字人民币钱包信息，采用在线方式通过线网中心系统向数字人民币的运营机构进行硬钱包的合法性校验，并完成进出站状态更新、行程匹配、乘车费用的计算等联机处理。

4.3.2 离线验证过闸

通过检票机内设的数字人民币 PSAM 卡对钱包有效性进行判断，同时也可以将乘客的进出站信息回写至钱包的乘客过程文件，从而可以依据 IC 卡近场支付流程完成硬钱包的操作，实现离线验证过闸。数字人民币硬钱包与 PSAM 卡由相同的发行机构发行。

5 对线网中心系统技术要求

5.1 基本要求

作为数字人民币业务在城市轨道交通售检票领域的统一入口，与受理银行机构共同处理数字人民币业务，统一接入并管理线网 AFC 系统的数字人民币支付和乘车功能。

统一对数字人民币应用的场景类型、支付方式、票卡类别进行定义。

在数字人民币硬钱包应用场景时，可使用现金、扫码和卡扣等形式进行补款。其中当使用数字人民币扫码和卡扣方式补款时，线网中心系统应对付款结果进行确认。

5.2 功能要求

对线网中心系统的功能要求如下：

a）具备联机数字人民币票卡处理功能。

b）具备数字人民币相关参数定义及下发、参数管理等功能，实现数字人民币票种、票价等参数化配置。

c）系统软件具备数字人民币数据处理功能，包括处理对数字人民币相关参数、交易数据、收益数据的上传下达和入库汇总统计功能等。

d）报表系统具备相关数字人民币应用统计、分析、查询、导出等报表功能。

e）密钥系统满足数字人民币的应用要求。

f）管理数字人民币支付方式的签约和解约数据；

g）管理数字人民币的支付绑定数据；

h）管理数字人民币的支付订单、校验和异常事务处理数据；

i）管理数字人民币支付方式和委托代扣数据。

j）具备定义数字人民币软钱包和硬钱包的在线或离线支付的功能，包括账户管理、订单管理、支付 URL 及确认、联机钱包有效性判断、OD 匹配等数据处理功能。

k）具备数字人民币交易的交易类型、交易数据格式、支付方式、票卡类型、清分检查规则、清分处理规则等的管理功能。

l）具备数字人民币交易文件分析功能，在文件中根据票卡特征进行区分。

m）具备数字人民币交易清分、对账功能。

n）具备数字人民币应用退款数据处理功能。

o）具备对数字人民币的交易明细、可疑、调整、拒付等数据处理功能。

p）本行业数字人民币交易数据流水号宜使用 BCD 编码格式，长度 8 字节，包含城市代码（2 字节）+扩展位（3 字节）+交易顺序编号（3 字节）（扩展位由各城市轨交自定义生成；交易顺序编号为单调递增字段）。城市代码（2 字节）采用行政区划代码（GB/T 2260）中的定义。

q）数字人民币硬钱包应用使用逻辑卡号为钱包唯一标识。

5.3 性能要求

前端设备请求超时响应时间不低于 500ms。

5.4 接口要求

与与数字人民币运营机构、线网 AFC 系统的账务接口和管理接口满足数字人民币的应用要求。

与受理银行机构存在管理和账务接口，实现离线、在线交易；与线网 AFC 系统存在管理和账务接口，共同进行轨道交通场景下票务应用的内部协调、一致运行；

与下位系统共同完成在线验证、实时交易同步或延时扣款。

6 对线路中央计算机系统及车站计算机系统技术要求

6.1 基本要求

对线路中心系统及车站中心系统的基本要求如下：

a）应保证本系统局域网联通，并与 AFC 线网中心以及终端设备间网络实现双向通信，满足数字人民币业务要求。

b）系统应具备 AFC 线网中心对数字人民币应用场景、支付方式、交易类型等业务功能要求。

c）系统应具备支持数字人民币在 TVM 上购票支付和充值，在 AGM 上进出站检票，在 BOM 上售票、充值、更新、退款等业务应用的功能。

d）系统应具备对终端设备上传的交易数据实现数据接收、发送、存储、票务处理和数据管理的功能。

6.2 功能要求

6.2.1 参数功能要求

对线路中心系统及车站中心系统的参数功能要求如下：

a）应能接收并保存上位系统下发的数字人民币相关参数，并能查询本地的数字人民币相关参数的版本，上报给上位系统。

b）应能向下位系统或设备同步数字人民币相关参数。

c）应能实时查询并获取下位系统或各终端设备数字人民币相关参数的版本，并上报，响应时间应满足设计要求。

d）应能自动识别上位系统发布的最新数字人民币应用相关的软件版本，并获取、存储、运行及反馈结果。

6.2.2 交易功能要求

对线路中心系统及车站中心系统的交易功能要求如下：

a）应能接收下位系统或设备上传的数字人民币相关交易数据，并保存到本地。

b）应能处理并上传保存在本地的数字人民币交易数据。

c）交易发送的时间间隔和数量上限应满足 AFC 系统离线交易传输设计要求。

6.2.3 对账功能要求

对线路中心系统及车站中心系统的对账功能要求如下：

a）应能统计和生成与数字人民币相关的客流和收益报表。

b）应能按照与 AFC 线网中心系统约定的机制核对交易数据的一致性。

6.3 性能要求

数字人民币相关业务处理和存储的性能指标，应满足 AFC 系统性能指标设计要求。

6.4 接口要求

对线路中心系统及车站中心系统的接口要求如下：

a）应按照与线网中心系统约定的接口机制，实现数字人民币相关业务，满足系统设计要求。

b）应按照线路系统与车站系统之间约定的接口机制，实现数字人民币相关业务，满足系统设计要求。

c）应按照与终端设备约定的接口机制，实现数字人民币相关业务，满足系统设计要求。

7 对车站终端设备技术要求

7.1 基本要求

对车站终端设备的基本要求如下：

a）车站终端设备应满足数字人民币在轨道交通自动售检票系统中的功能要求，按照数字人民币业务处理流程，实现数字人民币支付、查询、补票、退款、进出站等业务处理。满足数字人民币业务与 AFC 上位系统以及线网中心系统的通信及数据接口要求。

b）车站终端设备应实现数字人民币“软钱包”和“硬钱包”应用，支持小额支付、在线授权硬钱包过闸和离线验证硬钱包过闸的应用场景。

c）车站终端设备满足数字人民币在轨道交通自动售检票系统应用的环境要求，包括硬件兼容性和软件运行环境要求。

d）车站终端设备满足新增数字人民币票卡种类要求、设备管理要求、操作界面要求。

e）车站终端设备满足数字人民币跨地区互联互通的应用要求。

7.2 功能要求

对车站终端设备的功能要求如下：

a）参数处理

票种参数解析满足新增数字人民币票卡种类要求。

b） 业务处理

自动检票机根据数字人民币业务处理流程，实现数字人民币硬钱包进出站业务。

半自动售票机、自动售票机实现使用数字人民币软钱包进行支付的主扫或被扫功能。

半自动售票机、其他智能设备实现数字人民币软钱包及硬钱包行程及支付信息查询功能。

出现异常情况时，半自动售票机及其他客服设备能进行异常处理，实现数字人民币应用的补款、退款功能。

c） 界面要求

车站终端设备应满足数字人民币应用的乘客界面操作和提示要求，以及维护界面的设备管理要求。

7.3 性能要求

读写器对数字人民币硬钱包处理速度：每张小于等于 0.3s（包括识别、校验、编码等）；

自动检票机从检查数字人民币硬钱包有效性后，闸门完全打开时间小于等于 0.6s；

数字人民币软钱包支付操作响应速度性能要求应不低于其他互联网移动支付方式（如支付宝、银联支付等）性能要求。

通信正常的情况下设备的数字人民币数据能在 3s 内上传到车站计算机（SC）；

通信中断恢复后设备应能在 2min 内完成向 SC、ITP 上传未传送的数字人民币数据。

7.4 接口要求

7.4.1 与车站中心系统接口要求

满足车站中心系统定义的数字人民币业务相关非实时通信、时钟、参数、交易、状态、命令等接口要求。

7.4.2 与线网中心系统接口要求

满足线网中心系统定义的数字人民币业务相关实时通信、时钟、参数、交易、状态、命令等接口要求。

8 对通用读写器技术要求

8.1 基本要求

8.1.1 硬件要求

对通用读写器的硬件要求如下：

a）读写器硬件配置及材料要求须满足 T/CIITA 201.2-2021 的要求，当使用国产化 IC 芯片或操作系统时，性能指标不宜降低。

b）读写器能对符合 JR/T 0025-2018（3,5）和 ISO/IEC14443（2,3）TYPE A/B 标准的数字人民币硬钱包进行操作。

c）读写器具备通讯协议命令接口及 API，可对数字人民币运营机构发行的符合 ISO/IEC7816（1-4）标准的 SAM 卡进行操作；具有 RSA、DES、3DES、国密 SM1/2/3/4/5/6 等专用算法和安全数据专用硬件处理单元。

d）读写器实现数字人民币硬钱包和其他非接触 IC 卡的防冲突功能。

E）支持国产实时操作系统。

8.1.2 硬钱包票务处理流程模式要求

采用票务处理流程内置模式，读写器内置程序可以部分或全部实现 AFC 票卡业务逻辑，

实现数字人民币硬钱包的业务处理。

读写器接收上位机下发的业务指令，然后根据所述业务指令读取数字人民币硬钱包数据，并进行相应的业务处理。在离线验证场景下读写器可根据处理结果进行写卡操作，或者在在线验证场景下读写器可与上位设备进行数据交互处理。应能保存交易记录并在空闲时间将交易记录发送至上位机进行保存处理。本文中提到的数字人民币通用读写器作为数字人民币钱包的应用受理单元，适用于自动售票机（TVM）、半自动售票机（BOM）、自动检票机（AGM）、多功能自助票务终端（STM）、便携式检验票机（PCA）等车站终端设备。

8.1.3 二维码读头连接方式要求

设备二维码模块可以直接与工控机连接，也可以通过读写器与工控机连接。当通过读写器连接时，二维码模块采集的数据需经读写器转发给工控机，以完成数字人民币软钱包二维码小额支付业务的交易处理。。

8.2 功能要求

通用读写器主要实现数字人民币硬钱包在线验证和本地离线验证两种模式的进、出站检票以及异常处理（行政支付、退票）等功能。软钱包支付场景功能由设备二维码模块或者移动端 APP 实现。

8.2.1 软钱包支付场景功能要求

售票、补票类设备（如 TVM、BOM 等）支持采用数字人民币软钱包进行购票、充值、补票和退款等操作。AFC 系统内离线交易数据由读写器统一生成并逐层上传至线网中心系统。

8.2.2 硬钱包在线验证过闸场景功能要求

8.2.2.1 进站流程

读写器根据硬钱包过闸处理流程，实现硬钱包在线业务判断、获取预授权额度、记录进站信息、控制检票机通行等进站功能。

8.2.2.2 出站流程

读写器根据硬钱包过闸处理流程，实现硬钱包在线进站交易查询、行程判断、扣费处理、控制检票机通行等出站功能。

8.2.3 硬钱包离线验证过闸场景功能要求

8.2.3.1 进站流程

读写器根据硬钱包过闸处理流程，使用 PSAM 卡实现硬钱包离线行程有效性判断、行程文件更新，并控制检票机通行等进站功能。

8.2.3.2 出站流程

读写器根据硬钱包过闸处理流程，使用 PSAM 卡实现硬钱包离线进站信息判断、更新行程文件及控制检票机通行等出站功能，由线网中心系统向银行机构申请完成扣费。

8.2.4 异常处理功能要求

读写器须实现乘客在数字人民币硬钱包在线或离线认证模式下，遇到的异常情况导致不能正常进出站时，通过自助终端或半自动售票机进行异常处理的功能。主要包括：

a）通过查询行程信息或行程文件，分析异常原因。

b）可以对进出站顺序错误或余额不足等异常进行处理。

c）更新操作后，可正常进行出站，生成完整交易记录。

8.3 性能要求

对通用读写器的性能要求如下：

a）读写器整体性能指标符合 T/CIITA 201.2-2021 的要求。

b）数字人民币硬钱包读写时间：300ms（读写时间指从捕获到卡至卡交易过程数据读写全部结束的过程，包含读写过程中读写器的处理时间，不包含交易记录的产生及设备开门、出票等动作）。

8.4 接口要求

8.4.1 与终端设备的业务接口要求

a）商户钱包关联码查询，请求参数和响应参数。

b）预授权接口，请求参数和响应参数。

c）扣费接口，请求参数和响应参数。

d）数字人民币进站与出站匹配接口，请求参数和响应参数。

8.4.2 与车站终端设备的管理控制接口要求

a）初始化读写器通讯口，请求参数和响应数据。

b）读写器数字人民币业务控制接口，请求参数和响应数据。

c）状态查询接口，请求参数和响应数据。

d）同步时钟接口，请求参数和响应数据。

e）运营参数管理接口，请求参数和响应数据。

f）交易接口，请求参数和响应参数。

9 对软件系统技术要求

9.1 软件系统构成

数字人民币应用的关键构成包括数字人民币钱包、车站终端设备（含读写器）、线网中心系统以及外部运营机构。乘客通过使用数字人民币钱包在自动检票机完成进出站操作，系统连接线网中心系统及运营机构接口完成认证和扣费，在出现扣费失败等异常情况时，由半自动售票机进行补款、退票或黑名单解除申请等业务处理。系统构成应符合图 1 的规定。

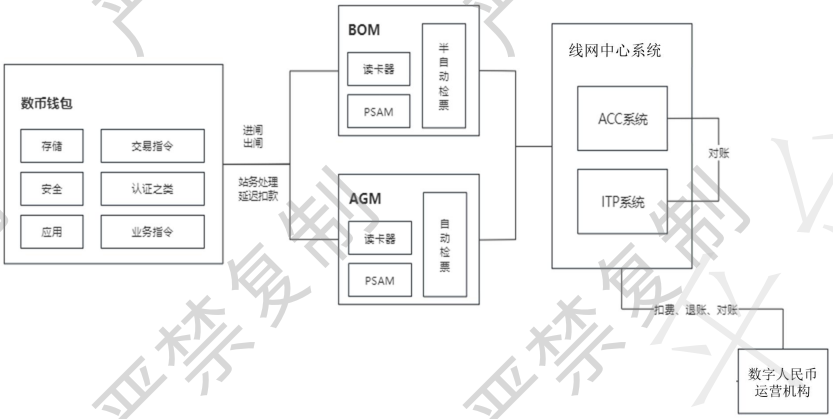

图 1 系统构成

9.2 软钱包支付场景软件要求

9.2.1 购票/充值

购票/充值业务流程应符合图 2 的规定。

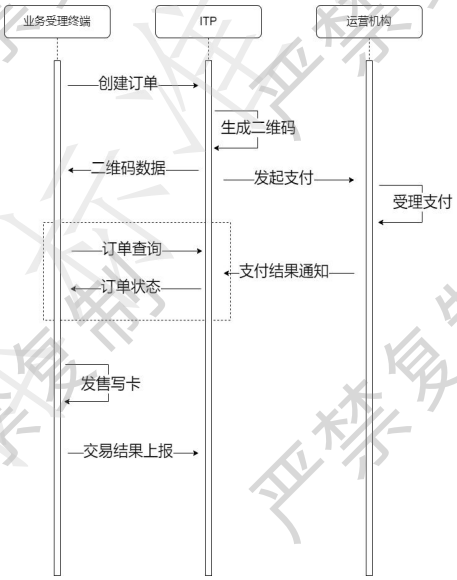

图 2 购票/充值流程

a）业务受理终端向 ITP 发起订单创建请求，向用户展示数字人民币付款码，引导用户完成支付；
b）业务受理终端向 ITP 轮询发起订单状态查询请求，检查订单是否已被支付；
c）当用户支付成功后，ITP 改变订单支付状态；
d）业务受理终端查询到订单已支付后，执行票卡发售/充值子流程；
e）业务受理终端发售成功后，向 ITP 发送发售/充值结果请求。

9.2.2 退票/退款

退票/退款业务流程应符合图 3 的规定。

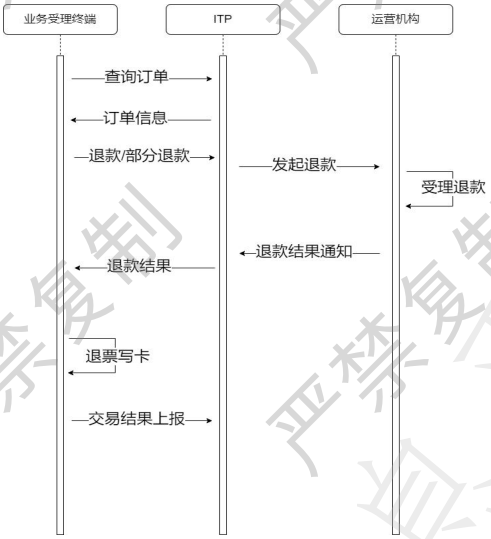

图 3 退票/退款业务

a）若在业务受理终端交易（发售、更新等）子流程处理过程中失败或部分失败，则业务受理终端应计算退还用户的金额；

b）业务受理终端向 ITP 发送订单查询请求，查询关联支付订单。根据订单号向互联网业务平台发起退款或部分退款请求；

c)若订单存在且未消费，业务受理终端应根据票务规则检查票/卡状态计算可退款金额，向 ITP 发起退款或部分退款请求；

d）成功后，业务受理终端完成票/卡的退票写卡子流程，并且保存相关交易信息；

e）支付系统向乘客数字人民币账户完成退款。

f）若失败，业务受理终端应提示失败信息或进行定时重试。

9.2.3 费用补缴

费用补缴业务流程应符合图 4 的规定。

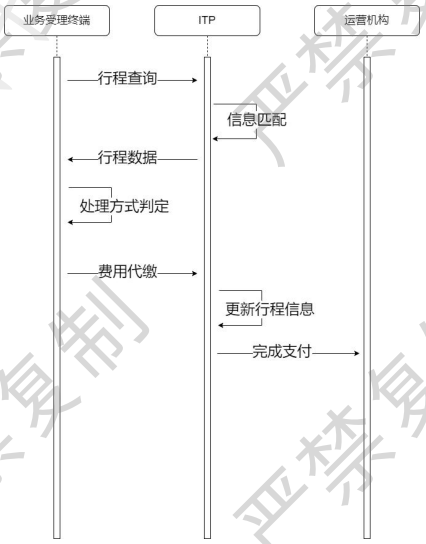

图 4 费用补缴

a）业务受理终端查询到待缴费行程后，提示乘客补缴行程费用；

b）乘客使用数字人民币硬钱包卡扣方式或软钱包扫码方式完成费用补款非现金支付，支付过程包括钱包编号、订单号等请求参数，以及包含返回信息的响应参数。

c）由数字人民币线上购得数字车票和线下购得实体车票，存在票务政策规定的需进行补缴行程费用时，可由上述方式进行 BOM 补款。

d）由非数字人民币购得车票，存在票务政策规定的需进行补缴行程费用时，可由上述方式进行 BOM 补款。

e）由数字人民币线上购得数字车票和线下购得实体车票，存在票务政策规定的需进行补缴行程费用时，可由现金进行 BOM 补款，补款信息需要与原数字人民币订单同步。

f）用户确认后，业务受理终端应向 ITP 发起补缴请求，完成更新操作。

9.2.4 账户异常费用补缴

账户异常费用补缴业务流程应符合图 5 的规定。

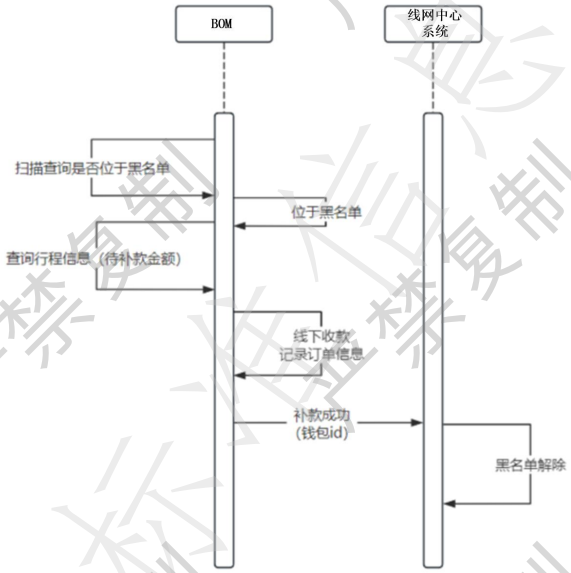

图 5 账户异常补款流程

a）数字人民币硬钱包离线验证过闸，后台扣费时账户余额不足列入黑名单，费用补缴后解除黑名单，乘客恢复使用数字人民币硬钱包过闸业务。

b）数字人民币硬钱包在线验证过闸，正常进站，在紧急模式或其他异常出站形成进站单边数据无法扣费，后补出站账户余额不足无法完成预授权，需费用补缴后可正常使用。

9.3 硬钱包过闸场景软件要求

9.3.1 在线验证过闸场景

a）在线验证模式下，数字人民币硬钱包进站时须进行资金冻结。ITP 完成用户鉴权后，向受理银行机构发起资金预授权申请，受理银行机构将资金锁定申请通过央行互联互通平台发送至付款银行机构，付款银行机构进行钱包状态、余额等信息校验，对符合锁定条件的数字人民币硬钱包进行金额锁定，ITP 收到金额锁定成功通知后开闸放行。锁定流程满足以下要求：

1）锁定金额应依据预计消费金额确定，锁定金额原则上应小于等于最大票价。

2）钱包可用余额小于锁定金额时锁定失败。

3）锁定金额对应具体订单，只限定对应订单支付使用。

4）受理订单号对应一笔锁定金额，扣款时受理订单号需与金额锁定受理订单号相

同。

5）锁定有效期应根据业务规则确定。

6）信息要素包括不限于锁定业务场景、受理订单号、付款钱包 ID、锁定金额、锁定有效期、商户编码、商户名称、是否需要开通小额免密、金额锁定状态、锁定失败原因。

b）在线验证模式下进站流程应符合图 6 的规定。

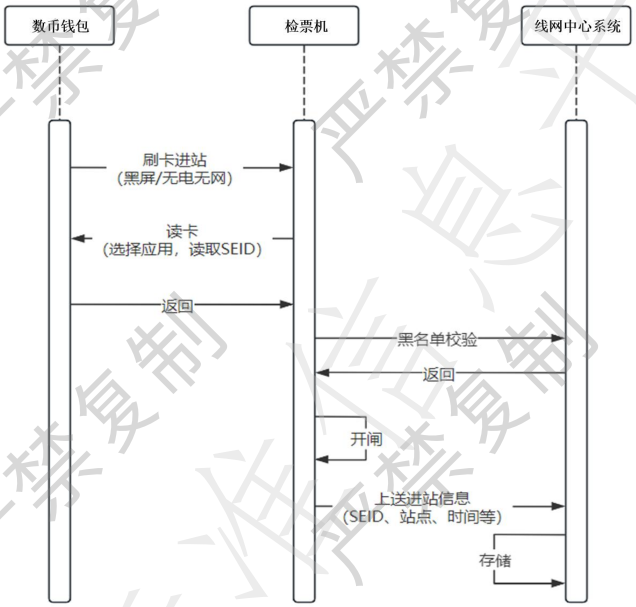

图 6 硬钱包在线验证进站流程

1）读写器读取硬钱包关联码，通过检票机连接 ITP 在线验证有效性，若无效，则不支持此银行机构数字人民币业务。

2）读写器读取数字人民币卡硬钱包信息，通过检票机按线网规程规定票价向 ITP 发起支付授权请求，并执行预授权操作，输出交易凭证（付款 token、卡唯一号、进站交易记录等）。

3）检票机调用 ITP 根据业务规则进行通行逻辑校验（行程 OD 状态等）、黑名单校验，若逻辑错误或在黑名单，则至 BOM 进行异常处理；

4）检票机根据运营机构的授权结果进行校验，检验通过后开闸放行；

5）检票机实时向 ITP 上传进站交易，ITP 保存。

c）在线验证模式下，用户出闸消费结束后，ITP 根据实际消费金额发起支付请求，受理订单号应与发起金额锁定填写的受理订单号一致。受理银行机构通过央行互联互通平台向付款银行机构发起收款请求，付款银行机构匹配锁定受理订单号，按实际金额付款，并将该笔业务剩余锁定金额解锁。如扣款失败，实现在锁定期内重复发起扣款，锁定有效期结束后，付款银行机构应自动解除锁定。

d）在线验证模式下出站流程应符合图 7 的规定。

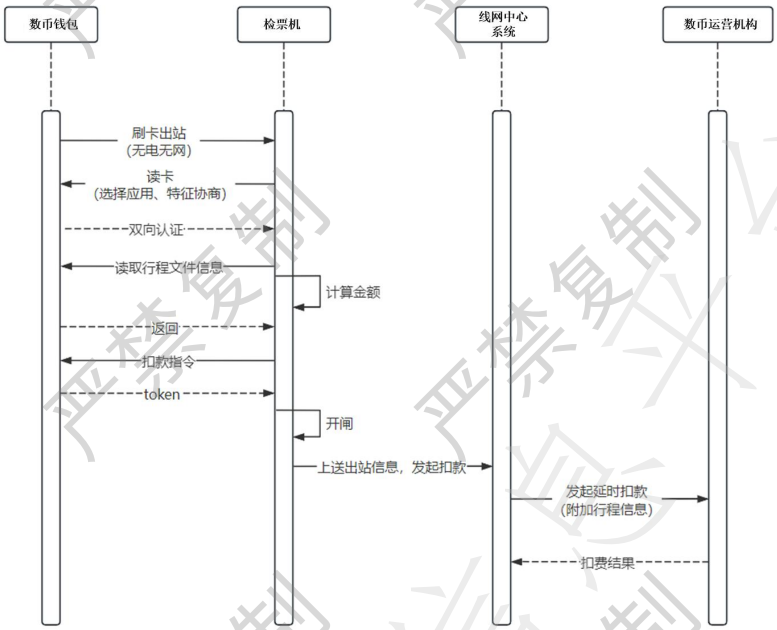

图 7 硬钱包在线验证出站流程

1）读写器读取硬钱包关联码，通过检票机连接 ITP 在线验证有效性；

2）检票机连接 ITP 判断行程信息是否正常，如果没找到匹配的进站交易记录，则不允许出站，需至 BOM 处理；

3）如果找到匹配的进站交易，则根据进站交易相关信息计算乘车费用，并进行预授权完成操作，完成实际车费扣费，并输出交易凭证（付款 token、卡唯一号、出站交易记录等）若不正常需至 BOM 处理；

4）检票机根据处理结果开闸放行，并向 ITP 上传出站交易；

5）ITP 应向运营机构发起授权完成请求，并记录支付结果，若支付失败更新黑名单。

e）在线验证模式下，在用户实际消费前，可以申请资金解锁。ITP 确认可以解锁后，发起解锁申请。受理银行机构通过央行互联互通平台发送至付款银行机构，付款银行机构匹配锁定记录，进行金额解锁，返回解锁结果并通知用户。满足以下要求：

1）付款银行机构收到解锁申请与原申请匹配一致后解锁。

2）对于同一钱包锁定多笔的，需逐笔解锁。

3）锁定资金在锁定有效期结束后，自动解锁。

4）解锁后不再受理银行机构对该笔锁定发起的扣款。

5）信息要素包括不限于原锁定受理单号、锁定业务场景、钱包 ID、商户编码、商户名称、金额解锁状态、解锁失败原因。

f）在线验证模式下，可以实现 ITP 向付款银行机构查询锁定处理状态。对于发送资金锁定申请未收到应答的情况，ITP 可发起资金锁定状态查询申请。付款银行机构收到资金锁定状态申请后，查询申请处理结果，并返回结果。信息要素包括不限于原锁定业务报文流水号、原申请日期、金额锁定状态、锁定失败原因。

9.3.2 离线验证过闸场景

a）离线验证模式下，用户出站时使用单离线延时可重复扣款流程。检票机通过识别付款方为数字人民币硬钱包并在完成多维度校验以后，根据数字人民币硬钱包行业文件中

读取的进、出站信息，自动计算票款生成付款信息，并将付款信息传送至 ITP，由 ITP 调用支付接口发起支付。由于存在数字人民币硬钱包扣费失败的情况，需要对同一个 token 能重复发起扣费动作，即补偿扣费流程。具体流程如下：

1）每次均需校验是否开通小额免密支付。

2）不校验交易顺序。

3）不比对交易实际发生时间与报文上送时间。

4）对于尚未取得成功应答的延迟联机交易，ITP 可以在订单有效期内，多次发起延迟联机交易。建议通过批量定时任务方式发起，订单有效期由数字人民币互联互通平台统一设置。

5）信息要素包括不限于商户号（代理商户号）、终端设备编号、随机字符串、支付订单号、商户订单号、订单金额、币种、订单生成时间、订单有效期、付款 token、渠道、交易模式、完成支付时间。

b）离线验证模式下进站流程

1）检票机通过读写器双向认证校验硬钱包有效性；

2）检票机调用 ITP 系统完成黑名单校验，若在黑名单中需至 BOM 处理；

3）乘客进站时，读写器读取数字人民币卡硬钱包的行程信息，并进行有效性进行判断（进出站标识）；若进出站标识为已进站，则不允许再次进站；若进出站标识为已出站，根据票务政策进行行程文件更新操作；

4）更新行程文件，同时保存进站交易记录（进站交易类型、交易时间、交易流水号、付款 token，卡唯一号等），开闸乘客进入车站付费区；

5）检票机传输进站信息给线网中心系统，线网中心系统进行存储。

c）离线验证模式下出站流程

1）检票机通过读写器双向认证校验硬钱包有效性；

2）检票机调用 ITP 系统完成黑名单校验，若在黑名单中需至 BOM 处理；

3）读写器读取数字人民币卡硬钱包的行程信息，并进行有效性判断（进出站标识）；若进出站标识为已出站，则不允许再次出站；若进出站标识为已进站，则根据行程信息计算乘车费用并向 ITP 和银行机构申请扣费，输出交易凭证（付款 token、卡唯一号等）；

4）更新行程文件（进出站标识更新为已出站），同时保存出站交易记录（交易类型、交易时间、交易流水号、付款 token，卡唯一号等）；

5）检票机将出站行程、扣款 token 信息传输给线网中心系统，开闸乘客出站。

d）离线验证模式下，对检票机发送完单离线付款操作指令后通讯中断产生的闪卡现象，须提示和满足用户重新刷卡。

e）离线验证模式中，数字人民币硬钱包所有指令处理时间应不超过 300ms。

9.4 硬钱包过闸异常处理软件要求

异常状况指乘客在使用数字人民币硬钱包进出站检票时，遇到的异常情况导致不能正常进出站，需要通过自助终端或半自动售票机进行异常处理的状况。

a）读写器读取数字人民币硬钱包唯一号，然后查询行程信息，分析异常原因。数字人民币硬钱包业务指令宜采用 BCD 格式编码。

b）如果在黑名单中，乘客通过现金或其他支付方式完成补款，通过 BOM 更新扣费订单状态为成功，将用户移出黑名单。

c）硬钱包在线验证过闸场景，若乘客在非付费区无法进站，查询最近一次乘车信息是

否余额不足导致行程未结束或出站交易不完整导致单边交易。按照票务规则，补缴上次的乘车费用或消除单边交易后再重新刷卡进站。

硬钱包离线验证过闸场景，若乘客在非付费区无法进站（进出站标识为已进站），先行更新行程文件补出站记录并补缴车费，生成补款交易记录；如果硬钱包余额不足，则需要人工进行数字人民币钱包充值，再行扣款并刷卡进站。进站异常处理业务流程应符合图 8 的规定。

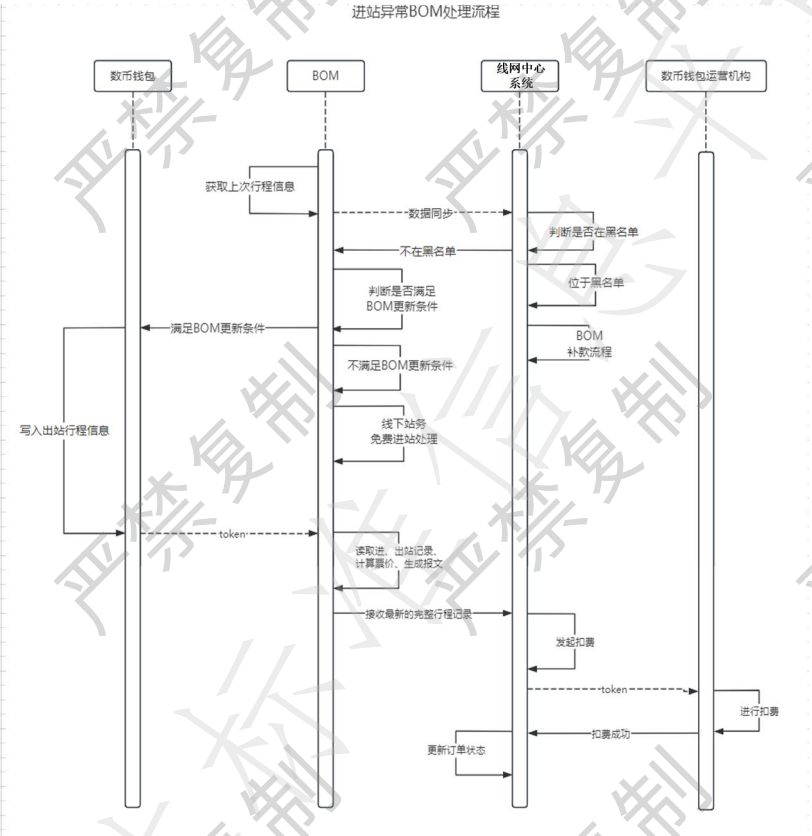

图 8 进站异常处理

d）硬钱包在线验证过闸场景，若乘客在付费区无法出站，查询进站行程信息，人工补充进站信息并根据票价政策设置预授权额度、执行预授权操作，输出交易凭证（付款 token 和卡唯一号），保存进站交易记录，然后正常刷卡出站。

硬钱包离线验证过闸场景，若乘客在付费区无法出站（进出站表示为已出站或非法闯入导致未正常进站），则根据票务政策进行扣费操作，更新行程文件（进出站标识更新为已进站），同时保存进站交易记录；乘客重新刷卡出站。出站异常处理业务流程应符合图 9 的规定。

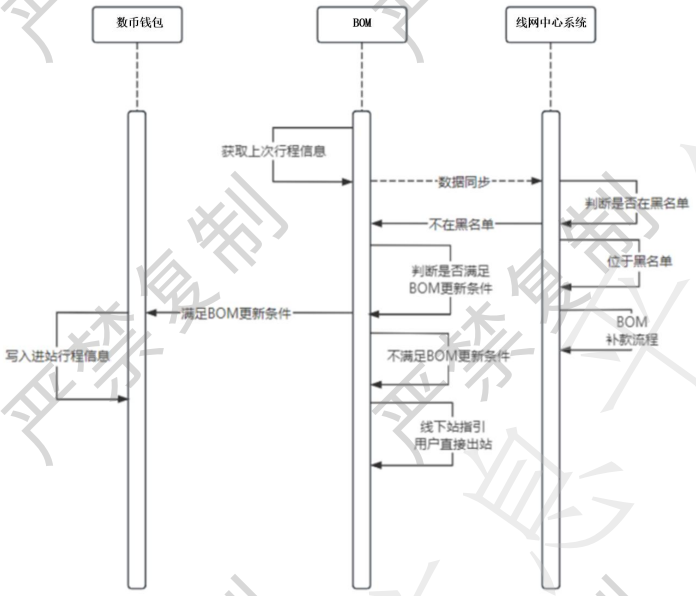

图 9 出站异常处理

10 对系统安全技术要求

10.1 安全与合规性要求

10.1.1 账户信息安全

系统应确保数字人民币应用中涉及的个人账户信息安全，符合《信息安全技术个人信息安全规范》等相关法律法规及要求。具体措施包括：

对账户信息进行加密存储，采用符合国家密码标准的加密算法，确保账户信息在存储和传输过程中的保密性。

严格控制账户信息的访问权限，仅授权的系统和人员才能访问账户信息，并对访问行为进行审计和记录。

定期对账户信息进行安全评估和漏洞扫描，及时发现并修复潜在的安全风险。

10.1.2 数字人民币信息安全

在数字人民币软钱包应用过程中，需对数据信息的完整性、真实性、不可抵赖性及时效性进行鉴别，对于未通过鉴别的非法数字人民币支付码将予以阻止。具体指标如下：

完整性：通过数据校验算法确保数字人民币数据在传输和存储过程中未被篡改；真实性：采用数字签名和证书验证机制，确保数字人民币数据来源于合法的运营机构或用户设备；不可抵赖性：通过数字签名和时间戳等技术，确保数字人民币交易行为的不可抵赖性，防止交易双方否认已发生的交易；时效性：设置合理的数据有效期和超时机制，确保数字人民币数据在有效期内有效，超时数据自动失效，防止重放攻击。

在数字人民币硬钱包应用过程中，离线验证模式时：数字人民币硬钱包在检票机前端应进行多维度校验，包括行业认证计数器校验、黑名单校验、行业标识校验、行业文件校验和基于 SM4 的 MAC 校验，PSAM 本地验证及记录行程文件性能应能符合各地轨道交通相关标准要求。

在线验证模式时，线网中心系统应将数字人民币硬钱包卡号通过联机交易发送至商户和

运营机构，由后台系统对数字人民币硬钱包合法性进行校验。

10.1.3 数据安全及风险控制

应采用电子安全交易技术，包括对称/非对称密钥算法、信息认证码（MAC）、数字签名、数字校验等，相关技术应符合国际、国家和行业技术标准及规范中有关交易安全的要求。线网中心系统与数字人民币运营机构之间的交易报文的加解密及认证规则，按照运营机构规则处理。

系统应对数字人民币交易进行实时监控和分析，识别可疑交易行为，采用用户行为分析、交易模式分析等技术手段，对频繁大额交易、异常交易频率等进行监测，通过单笔交易限额，根据钱包类型分级控制（如一类钱包每笔小于等于 5000 元，四类钱包每笔小于等于 1000 元），防范洗钱风险。

10.1.4 认证安全

系统应采用多因素认证机制，对用户身份进行严格认证，确保用户身份的真实性和合法性。具体要求包括：

a）对接入系统的设备和终端进行身份认证，确保接入设备的合法性和安全性。

b）定期对认证机制进行评估和更新，确保认证机制的有效性和安全性。

10.1.5 合规性要求

系统的设计和运行应符合国家相关法律法规和监管要求，具体要求包括但不限于：

a）定期进行合规性评估，确保系统在运营过程中持续符合法律法规和监管要求。

b）建立合规性管理制度，明确合规性责任和流程，确保系统运营过程中的合规性。

c）支付终端需符合中国人民银行数字货币研究所的合规要求。

d）系统需支持监管机构穿透式查询（如可疑交易追溯）。

10.2 接口安全要求

10.2.1 对内接口安全

应满足对数字人民币参数、交易数据等数据传输的安全要求，实现内部数据交互安全。

采用加密传输协议（如 TLS/SSL）对内部接口数据进行加密传输，防止数据在传输过程中被窃取或篡改。进行严格的访问控制和认证，仅授权的系统和人员能够访问内部接口。

10.2.2 对外接口安全

应满足对数字人民币业务相关签约、支付、查询等接口的安全要求，实现对外数据交互安全。

采用数字签名和加密等安全机制，确保数据的完整性和保密性。进行严格的权限管理和认证，仅授权的用户和系统能够访问对外接口。

10.3 管理安全要求

系统应从安全管理制度、安全管理机构、人员安全管理、系统建设管理和系统运维管理等方面进行管理安全保障，具体要求如下：

安全管理制度：建立完善的安全管理制度，明确安全责任和流程，确保系统安全运行。

安全管理机构：设立专门的安全管理机构，负责系统的安全管理和监督工作。

人员安全管理：对系统管理和操作人员进行安全培训和考核，确保人员具备必要的安全意识和技能。

系统建设管理：在系统建设过程中，严格按照安全标准进行设计、开发和测试，确保系统的安全性。

系统运维管理：建立系统运维管理制度，定期对系统进行安全检查和维护，及时发现和处理安全问题。