ICS xx.xx

L xx.xx

**团体标准**

CIITA 204-2024

xxxx-xx-xx 发布

xxxx-xx-xx 实施

中国信息产业商会 发布

**数字人民币在轨道交通自动售检票系统**

**中的应用**

**(征求意见稿）**

**目 次**

[前 言 4](#_Toc9003)

[引 言 5](#_Toc31134)

[数字人民币在轨道交通自动售检票系统中的应用 6](#_Toc11490)

[1 范围 6](#_Toc2349)

[2 规范性引用文件 6](#_Toc1081)

[3 术语、定义和缩略语 6](#_Toc19649)

[4 数字人民币在AFC系统中的应用概述 9](#_Toc18897)

[4.1 支付场景 10](#_Toc920)

[4.2 检票场景 10](#_Toc25743)

[5 数字人民币业务在AFC线网中心的要求 11](#_Toc29493)

[6 数字人民币业务在AFC线路中心及车站中心系统的要求 12](#_Toc23892)

[6.1 功能要求 12](#_Toc7353)

[6.2 接口要求 12](#_Toc25971)

[6.3 性能要求 13](#_Toc13817)

[7 数字人民币业务在AFC互联网业务平台的要求 13](#_Toc17911)

[7.1 总体要求 13](#_Toc19513)

[7.2 数字人民币业务在AFC支付场景中的应用要求 14](#_Toc9716)

[7.3 数字人民币业务在AFC过闸通行场景中的应用要求 16](#_Toc26028)

[8 数字人民币业务应用于AFC专用设备的要求 18](#_Toc18549)

[8.1 基本要求 18](#_Toc24632)

[8.2 数字人民币业务在支付场景于专用设备的要求 19](#_Toc9926)

[8.3 数字人民币业务在过闸场景于专用设备的要求 21](#_Toc32521)

[8.4 接口要求 23](#_Toc12844)

[8.5 性能要求 23](#_Toc26095)

[9 数字人民币业务在AFC通用读写器的要求 23](#_Toc8269)

[9.1 总体要求 23](#_Toc30894)

[9.2 数字人民币业务支付场景于读写器的要求 24](#_Toc32719)

[9.3 数字人民币业务过闸场景于读写器的要求 24](#_Toc1428)

[9.4 与ITP接口要求 26](#_Toc32504)

[9.5 技术指标 27](#_Toc7713)

[10 数字人民币业务AFC应用软件要求 27](#_Toc23643)

[10.1 数字人民币业务支付场景的应用软件要求 28](#_Toc21886)

[10.2 数字人民币业务过闸场景的应用软件要求 30](#_Toc31184)

[10.3 接口要求 32](#_Toc7188)

[10.4 性能要求 32](#_Toc3148)

[10.5 软件系统安全性要求 32](#_Toc26762)

[11 数字人民币业务系统对运行环境及性能的要求 33](#_Toc30545)

[11.1 可靠性要求 33](#_Toc8680)

[11.2 安全性要求 33](#_Toc6416)

[11.3 扩展性要求 34](#_Toc7101)

[11.4 可维护性要求 34](#_Toc13432)

[11.5 兼容性要求 34](#_Toc15473)

[11.6 合规性要求 34](#_Toc20668)

[11.7 接口要求 34](#_Toc26411)

前 言

本标准按照 GB/T 1.1-2020 给出的规则起草。

本标准由中国信息产业商会自动售检票专业委员会提出。

本标准由中国信息产业商会归口。

本标准起草单位：......。

本标准主要起草人：…，…。

引 言

随着数字人民币应用在轨道交通场景中的业务流程不断完善，数字人民币已成为轨道交通数字经济中不可或缺的重要一环。一方面能够促使地铁行业逐步实现智能化、自动化，推动地铁行业的数字化转型；另一方面可以降低地铁出行的支付门槛，使更多人能够享受到便捷、安全的出行服务。

目前阶段，数字人民币与地铁通行设备之间在支付方式、安全性、效率等方面均未实现统一标准。支付方式的标准定义涉及数字人民币在地铁闸机、自动售票机等设备上的识别与交易流程，统一标准可以解决不同设备或系统间存在的兼容性问题，改善乘客支付体验；安全性的标准定义是保障数字人民币交易过程中数据安全、防止欺诈行为的关键，统一标准可以减少安全漏洞，降低乘客资金风险；效率性的标准定义涉及数字人民币支付的速度和稳定性，统一标准可以解决支付流程繁琐、速度慢、甚至支付失败的情况，提高地铁通行效率。

本《数字人民币在AFC系统的应用》团标将作为建设AFC系统的指导性文件，是对《城市轨道交通自动售检票系统》（T/CIITA201-2021）标准的补充和数字人民币在轨道交通自动售检票系统中的应用标准化空白的填补。通过《数字人民币在AFC系统的应用》的实施，将能够进一步提升AFC系统的自主创新能力，推动轨交AFC行业发展。

数字人民币在轨道交通自动售检票系统中的应用

# 范围

本文件规定了数字人民币应用在轨道交通自动售检票系统中与线网清分系统、互联网票务系统、（多）线路中心系统、车站系统、专用设备售检票设备、读写器的技术关系以及实现方式；规定了数字人民币“软钱包”和“硬钱包”的技术形态，以及软钱包小额支付、在线授权硬钱包过闸和离线验证硬钱包过闸的应用场景，以及相对应的业务流程；规定了数字人民币在轨交售检票系统应用的运行环境要求、安全要求以及接口兼容性要求。

本标准适用于轨道交通及周边交通系统（公交、市域铁路等）在进行AFC系统设计、建设、运营和改造过程中，应用数字人民币作为支付方式或过闸方式时，作为设计、实施、评审和检验的指导文件。

# 规范性引用文件

下列文件对于本文件的应用是必不可少的。凡是注日期的引用文件，仅所注日期的版本适用于本文件。凡是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 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/CAMET 11002 《城市轨道交通云平台构建技术规范》

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》

中国人民银行数研所 《数字人民币硬钱包轨交延迟交易技术方案》

# 术语、定义和缩略语

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。

2.车站计算机系统 station computer

管理车站的票务、运行、客流统计等的计算机系统。

3.金融IC卡

由各银行发行的卡面印有银联及闪付标识的芯片银行卡（含借记卡、信用卡），或承载金融IC卡信息的移动设备（如手机Pay、可穿戴设备等）。

4.线网最高单程票价

指轨道交通线网普通车厢最高单程票价。

5.线网最低单程票价

指轨道交通线网普通车厢最低单程票价。

6.运费

提供线路运营服务的运营商为乘客提供乘车服务所得的运输服务收入。

7.系统后台中交易记录信息不完整

相对于交易记录完整性，各种车票出现某项信息缺失时，即视为交易记录信息不完整。

8.逾期交易

因通信故障等原因造成交易数据无法按时上传，超过滞留上限天数的交易数据，称为逾期交易。

9.备份交易

交易数据丢失备份回来的数据。

10.灰交易

在复杂型读写器对储值卡以非接触方式进行读写的过程中，由于环境的不稳定性造成卡片数据和实际交易数据缺失或不一致的一类交易。

11.票款冲减

对已结算、有问题的数据进行提取、置负的过程。本计算结果不影响已结算结果，可计入下一结算日或补加结算单。

12.车站计算机系统

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。

13.车站终端设备

安装于各轨道交通线路车站，并进行车票发售、进站检票、出站检票、充值、验票分析等读写交易处理的终端设备。

14.自动检票机

对车票进行检验和处理，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。

15.半自动售票机

用于车站工作人员使用，并提供车票的发售、赋值、补充、更新、退款等业务处理功能的设备。

16.自动售票机

用于车站向乘客提供自助购票并赋值有效车票功能，并具备自动处理支付和找零功能的设备。

17.自助票务处理机

用于车站向乘客提供票务自助处理、信息咨询服务、开具电子发票等功能，能替代车站票务客服人员及票房售票机、自动验票机的大部分工作量。

18.运营机构（运营商）

负责数字人民币发行、运营和管理的银行或其他金融机构。

19.商户

使用数字人民币业务的单位或个人。

缩略语

下列缩略语适用于本文件。

|  |  |  |
| --- | --- | --- |
| 缩略词 | 英文全称 | 中文解释 |
| AFC | Automatic Fare Collection | 自动售检票系统 |
| ACC | AFC Clearing Central | 轨道交通票务清分中心 |
| MLC | Multiple Line Center System | 多线路中心 |
| CLC | Cluster Line Center | 多线路中央计算机系统 |
| ITP | Internet Ticket Platform | 互联网票务管理系统 |
| SLE | Station Level Equipment | 车站终端设备 |
| SC | Station Computer System | 车站计算机系统 |
| FTP | File Transfer Protocol | 文件传输协议 |
| IPS | Intrusion Prevention System | 入侵防御系统 |
| IP | Internet Protocol | 互联网协议 |
| NOCC | Net Operating Control Center | 网络运营控制中心 |
| AGM | Automatic Gate Machine | 自动检票机 |
| SAGM | Side Automatic Gate Machine | 边门检票机 |
| BOM | Booking Office Machine | 半自动售票机 |
| TVM | Ticket Vending Machine | 自动售票机 |
| STM | Self-service Ticketing Machine | 自助票务处理机 |
| PCA | Portable Card Analyzer | 便携式检验票机 |
| MST | Mobile Sell Ticketing Terminal | 移动票务终端 |
| ITM | Inelligent Ticketing Machine | 智能票务终端 |
| SAM | Secure Access Module | 安全存取模块 |
| iTVM | Internet Ticket Vending Machine | 互联网售票机 |
| MAC | Message Authentication Code | 报文鉴别码 |
| SAM | Secure Authentication Module | 安全认证模块 |
| ATC | Application Transaction Counter | 应用交易计数器 |
| SE | Secure Element | 安全单元 |
| MTBF | Mean Time Between Failure | 平均无故障工作时间 |
| MTTR | Mean time to repair | 平均修复时间 |
| token | Tokenization | 令牌 |
| NFC | Near Field Communication | 近场通信 |
| HCE | Host-based Card Emulation | 基于主机的卡模拟 |
| TEE | Trusted Execution Environment | 可信执行环境 |
| H5 | HyperText Markup Language 5 | 构建Web内容的一种语言描述方式 |
| OD | ORIGIN and DESTINATION | 交通出行数据 |
| IC | Integrated Circuit | 集成电路 |
| PSAM | Purchase Secure Access Module | 销售点终端安全存取模块 |
| RSA | Rivest、SharmirAdleman | Rivest、Sharmir和Adleman提出的一种非对称密钥算法 |
| DES | Data Encryption Standard | 数据加密标准 |
| SM2 | PublicKey Cryptographic Algorithm SM2 Based on Elliptic | SM2椭圆曲线公钥密码算法 |
| SM3 | SM3 Cryptographic Hash Algorithm | SM3密码杂凑算法 |
| SM4 | SM4 Cryptographic Algorithm | SM4分组密码加密算法 |
| URL | Uniform Resource Locator | 统一资源定位器 |
| PSAM | Purchase Secure Access Module | 销售点终端安全存取模块 |
| RSA | Rivest、SharmirAdleman | Rivest、Sharmir和Adleman提出的一种非对称密钥算法 |
| DES | Data Encryption Standard | 数据加密标准 |

# 数字人民币在AFC系统中的应用概述

数字人民币钱包是数字人民币的载体，可以分为软钱包和硬钱包。软钱包基于移动支付APP、软件开发工具包（SDK）、应用程序接口（API）等为用户提供服务；硬钱包基于安全芯片等技术实现数字人民币相关功能，依托IC卡、手机终端、可穿戴设备、物联网设备等为用户提供服务，软硬钱包结合丰富了AFC应用场景中的钱包生态体系，满足不同需求。

## 支付场景

### 软钱包支付

#### 线上购票

乘客线上通过轨道交通App购票时，点击需要购买的车票，选择支付方式为数字人民币，输入支付密码后即可出票。

使用数字人民币线上支付前，需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。签约可通过为子钱包推送、轨道交通App端 H5 直连和轨道交通App端 API 直连三种方式。

可以生成二维码支付凭证也可以使用TVM领取实体车票。

#### 线下购票

乘客使用移动终端通过数字人民币软钱包扫描 AFC 终端设备上提示的二维码，完成购票。

乘客使用移动终端展示数字人民币软钱包上的付款二维码，通过被 AFC 终端设备扫描方式完成购票。

### 乘车码过闸数字人民币支付

进站前，打开轨道交通App，选择支付方式为数字人民币支付。

进站时，自动检票机扫描轨道交通乘车码方式进站。

出站时，自动检票机扫描轨道交通乘车码方式出站。轨道交通App收到乘客的消费记录，通过合作银行提供的电子钱包代扣支付申请接口发起代扣申请，合作银行接收代扣申请，将用户出行消费款从用户个人数字人民币账户代扣到轨道交通电子钱包账户。

## 检票场景

### 数币子钱包检票场景（在线验证）

进站前，乘客申请数字人民币硬钱包。

进站时，乘客使用数币子钱包置于闸机读写器处，读写器读取数币子钱包信息，向运营机构在线进行有效性判断，申请预授权，根据票价政策，判断额度充足时允许进站（余额不足不放行），并后台记录。

出站时，乘客使用数币子钱包置于闸机读写器处，读写器通过闸机在线连接后台确认合法性，并在行程匹配后扣款，扣费token回传运营机构确认后，扣费记录再返回AFC系统至闸机生成交易。扣款由ITP后台对应运营商中帐户母钱包扣除，返回闸机生成交易数据再上传，不对数币子钱包进行更新写操作。

### 硬钱包检票场景（本地离线验证）

乘客使用开通包含乘客过程文件区的数币硬钱包过闸，闸机内需设置数字人民币PSAM卡，数币硬钱包与PSAM卡由相同的发行机构发行。

乘客进出站时，行程信息写入钱包的乘客过程文件区，读写器通过PSAM卡对钱包有效性进行有效性判断。在出站时通过对钱包内形成文件的判断，由后调行运营机构提请本账户扣费操作，扣费操作token在运营方进行备案确认，并回传AFC系统至闸机。行程不完整或其它票务异常操作，需在BOM上进行异常处理。

PSAM本地验证及记录行程文件性能应能满足各地轨道交通相关标准要求。

### 双离线场景

双离线检票场景中数字人民币验证及扣费操作由终端设备和硬钱包直接操作完成，此场景结合技术发展、政策完善进一步研究。

# 数字人民币业务在AFC线网中心的要求

1. AFC线网中心统一管理线网中心AFC系统的数字人民币支付、乘车功能，为乘客提供多元化乘车支付体验，进一步增强公共交通出行的便利性。

2. AFC线网中心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。

3. AFC线网中心具备定义数字人民币在线或离线支付的功能，实现硬钱包或软钱包方式，包括支付订单管理、支付URL及确认、联机钱包有效性判断、0D匹配等数据处理功能。具体功能包括：

管理数字人民币支付方式的签约和解约定义数据和交易数据；

管理数字人民币的支付绑定数据；

管理数字人民币的支付订单、校验和异常事务处理数据；

管理数字人民币支付方式和委托代扣数据。

1. AFC线网中心具备数字人民币票卡处理功能。

线网中心对数字人民币交易的交易类型、支付方式、票卡类型、清分检查规则、清分处理规则等具备编辑功能。

线网中心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，交易格式满足相关业务要求。

线网中心对数字人民币交易的票卡交互流程满足相关业务处理规范要求。

线网中心对数字人民币交易具备客流统计功能，统计进、出站等客流，交易格式满足客流处理规则。

线网中心对数字人民币交易具备清分、对账功能，交易业务流程和交易格式满足相关业务清分、对账处理规则。

1. AFC线网中心具备数字人民币签约、解约数据管理功能。
2. AFC线网中心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。
3. AFC线网中心具备数字人民币交易数据管理功能，统一定义数字人民币交易数据格式。

8. AFC线网中心具备数字人民币退款数据处理功能。

9. AFC线网中心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。

10. AFC线网中心报表系统具备相关数字人民币统计、分析、查询、导出等报表功能。

11. AFC线网中心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。

12. AFC线网中心具备数字人民币相关交易数据管理功能。

13. AFC线网中心密钥系统满足数字人民币的应用。

14. AFC线网中心与内、外部系统的接口满足数字人民币的应用。

# 数字人民币业务在AFC线路中心及车站中心系统的要求

## 功能要求

### 一般规定

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。

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。

系统应具备数字人民币在AGM上的进出站检票业务功能。

系统应具备数字人民币在TVM上的购票支付和充值业务功能。

系统应具备数字人民币在BOM上的售票、充值、更新等支付业务和退票的退款业务功能。

### 参数功能要求

应能接收上位系统下发的数字人民币相关参数，并保存到本地。

应能查询本地保存的数字人民币相关参数的版本。

应能向下位系统或设备同步数字人民币相关参数。

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。

应能将本地保存的数字人民币相关参数版本，上报给上位系统。

### 交易功能要求

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。

应能处理并上传保存在本地的数字人民币交易数据。

交易发送的时间间隔和数量上限应满足设计要求。

### 对账功能要求

应能统计和生成与数字人民币相关的客流和收益报表。

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。

## 接口要求

应按照与票务清分系统约定的接口机制，实现数字人民币相关业务，应满足系统设计要求。

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，应满足系统设计要求。

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，应满足系统设计要求。

## 性能要求

系统在规划设计阶段，应设定数字人民币相关业务的性能指标，并按设定的性能指标进行系统设计。

# 数字人民币业务在AFC互联网业务平台的要求

## 总体要求

1.互联网业务平台（ITP，Internet Ticketing Platform）作为数字人民币业务在轨道交通领域的统一入口，承担与受理银行机构和上位系统的联机交易功能，满足数字人民币作为互联网通行凭证和支付手段在轨道交通场景中的应用。

2.ITP与受理银行机构存在管理和账务接口，支持离线、在线交易；与线网中心系统存在管理和账务接口，共同保证轨道交通场景下票务应用的内部协调、运行一致性；与下位系统共同完成在线验证、实时交易同步或延时扣款。

3. ITP应充分考虑前端设备的请求超时响应时间，避免超时响应时间设置过小，导致前端设备由于无法获取返回信息而产生异常。超时时间应依据ITP总体架构、组件型号、系统版本进行设置，超时响应时间不低于500毫秒。

4. 建议对本行业数币交易数据流水号生成规则进行统一，各城市轨交应共同维护并保证交易流水号的唯一性。轨道交通交易流水号生成规则建议使用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）。在有硬钱包应用场景时，建议使用数字人民币硬钱包轨交行业计数器。

5. 数字人民币硬钱包应用进行交易和业务处理时，使用逻辑卡号为钱包唯一标识，并且在BOM、STM等设备前端页面显示。

6. 数字人民币硬钱包应用场景应支持现金、扫码、卡扣等形式补款。使用数字人民币扫码和卡扣方式补款时，ITP应对付款结果进行确认，避免发起付款成功但由于硬钱包余额不足等原因，造成实际未扣款成功，而前端误认为已扣费的情况。

7. 采用“延时扣费”模式的ITP后台，应根据当地轨道交通票务规范，对于“有进无出”、“有出无进”等单边情况完善黑名单管理机制和单边交易处理流程。

8. 数字人民币硬钱包业务指令采用BCD格式编码，ITP须充分考虑字段编码规则，对存在使用字母编码的字段统一进行约定，避免转码异常。

## 数字人民币业务在AFC支付场景中的应用要求

### 基本要求

1.ITP应实现在TVM、BOM、STT等设备使用数字人民币软钱包主扫或被扫的方式，购买单张或多张车票，以及对交通一卡通、交通联合卡等进行充值的应用。

2.ITP应实现在BOM使用数字人民币软钱包进行补款、退款的操作；实现在BOM对数字人民币硬钱包进行补行程的操作。

3.在进行查询、补款或退款操作时，BOM可请求ITP获取数字人民币硬钱包状态。请求参数包括不限于钱包编号、交易类型（进站、出站）、钱包银行、钱包介质（HEC、TEE、SIM卡、IC卡等）、手机号码。响应数据包括不限于返回码、返回信息、钱包状态（初始化、已进站、已出站、补进站、补出站、超时出站、XX时间内免费更新、黑名单等）、上次交易处理时间、商户银行协议号、上次交易车站。

4.在进行硬钱包补行程操作时，BOM可请求ITP获取数币钱包账户信息。请求参数包括不限于命令码、当前车站编号、当前设备编号、当前车站模式、设备测试状态、当前日期时间、物理卡号。响应参数包括不限于返回码、票卡类型、ATC、钱包关联码、交易索引、母钱包ID、时间戳、管理操作类型、消息认证码。

5.在进行补款操作时。BOM可请求ITP查询数字人民币硬钱包欠费记录。请求参数包括不限于钱包编号、返回码、返回信息、欠费金额、欠费行程等。

### 售票、充值订单管理要求

1、请求生成单程票订单。请求参数包括不限于起点站点代码、终点站点代码、票价、购买数量、购票方式（按站点购票、按固定票价购票等）、支付方式（数字人民币等）。响应参数包括不限于返回码、返回信息、订单号、二维码信息。

2、TVM充值下单请求。请求参数包括不限于票卡逻辑号、票卡物理号、充值前金额、请求交易金额、支付方式（数字人民币等）。响应参数包括不限于返回码、返回信息、订单号、二维码信息。

3、ITP提供所有支付订单的查询，通过主动查询订单状态，完成下一步的业务逻辑。调用查询接口要求如下：

①ITP、网络、服务器等出现异常，ITP最终未接收到支付通知。

②调用支付接口后，返回系统错误或未知交易状态情况。

③调用被扫支付API，返回“处理中”的状态。

④调用关单或撤销接口API之前，需确认支付状态。

⑤信息要素包括不限于商户号（代理商户号）、终端设备编号、支付订单号、商户订单号、订单状态、订单金额、币种、渠道、交易模式。

### 补款管理要求

1.数字人民币欠费补款非现金下单。请求参数包括不限于钱包编号、操作员编码、班次序列号、操作流水号、交易金额、欠费行程。响应参数包括不限于返回码、返回信息、订单号。

2.数字人民币钱包非现金补款扫码支付。请求参数包括不限于订单号、支付渠道编码、支付渠道账号认证码。响应参数包括不限于返回码、返回信息。

3.数字人民币钱包欠费现金补款结果通知。请求参数包括不限于钱包编号、操作员编码、班次序列号、操作流水号、交易金额、欠费行程、操作结果通知。响应参数包括不限于返回码、返回信息。

4.数字人民币钱包欠费重试扣费主动触发。请求参数包括不限于钱包编号。响应参数包括不限于返回码、返回信息。

### 退款管理要求

1、当交易发生之后一段时间内需要退款时，ITP可以通过退款接口将支付款退还给用户，支付系统将在收到退款请求并且验证成功之后，按照退款规则将支付款按原路退到用户账号上。需要注意以下几点：

①交易时间超时的订单无法提交退款。

②退款满足单笔交易分多次退款，多次退款需要提交原支付订单的订单号和设置不同的退款单号。

③申请退款总金额不能超过订单金额。

④每个支付订单的部分退款次数不能超过一定次数。

⑤信息要素包括不限于商户号（代理商户号）、支付订单号、商户订单号、退款单号、订单金额、退款金额、退款原因、退款渠道。

2、提交退款申请后，ITP须可以查询退款实时状态，退款有一定延时。信息要素包括不限于商户号（代理商户号）、支付订单号、商户订单号、退款单号、订单金额、退款金额、退款渠道、退款状态、退款成功时间。

### 对账管理

ITP每天定时上送前一天的数字人民币交易文件到ACC的FTP对应目录下。若某一天的文件缺失，应实现重新生成。ITP数字人民币交易文件结构格式定义包括文件头和文件体。ITP数字人民币对账文件结构包括文件头、文件体和校验码。文件头包括不限于文件类型、文件生成时间、文件版本、文件记录数。文件体包括不限于运营日期、票卡逻辑号、交易日期时间、票卡计数器、交易类型、车票主类型、车票子类型、支付方式、交易金额、优惠金额、当前车站代码、设备编码。

## 数字人民币业务在AFC过闸通行场景中的应用要求

### 基本要求

1.数字人民币硬钱包业务在AFC过闸通行场景中存在两种模式，离线验证模式和在线验证模式。各地轨道交通机构应充分结合自身系统架构特点、计费方式、付费手段、账务规则、业务流程等方面，选择适配性、高效性、兼容性更优的模式建设。

2.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；在线验证模式中，数字人民币硬钱包所有指令和交易处理时间由通讯时间、后台响应效率等因素决定。

3.为保证数字人民币硬钱包应用的兼容性及扩展性，应统一使用[中国人民银行数字货币研究所](http://www.baidu.com/link?url=I_431wZ762Zr6S673lsbwvuqwYjwdhAN3y7O-azRWufIlHD8PfyaThenL_fwqtthHzel1t4Wjr1zUmSu4Ubgn8ML37jvWblUmq-dG7BySBOmbevr7SaM9yU8NXE2JqXXV_foB9ZL3G-_G6ADaNwxvO1R1DgCBzvEixilLjtcUvTje2nFvU8EbKQrMVaaqF8uCDbzif3ONtC3AA3K0D6doTejYO9EuXFBrAt2ERyPzHy" \t "https://www.baidu.com/_blank)正式申请的AID。

4.在特征协商时，轨道交通机构应根据交易模型、终端形态、联网能力、行业标识等，从匹配的交易模型中选择最优交易模型。

5.离线验证模式中，数字人民币硬钱包在闸机前端须进行多维度校验，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；在线验证模式中，ITP需要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进行校验。

6.对于校验成功的数字人民币硬钱包，离线验证模式中，闸机须将进、出站信息写入数字人民币硬钱包的行业文件中；在线验证模式中，ITP须将进、出站信息计入后台数据表中。

7.此两种模式下，ITP应能接收地铁终端设备上传的数字人民币钱包乘车行程信息,包括不限于交易类型（进站、出站、超时出站等）、设备类型、票卡类型、钱包编号、手机号码、所属银行机构、数字人民币钱包扣费token、钱包介质（HEC、TEE、SIM卡、IC卡等）、SEID、闸机交易时间、闸机交易车站代码、实际交易金额、超时金额、设备ID、钱包状态（初始化、已进站、已出站、补进站、补出站、超时出站、XX时间内免费更新等）、闸机处理结果、上次交易车站代码、票卡计数器、上次交易时间。

### 数字人民币硬钱包过闸离线验证模式

1、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。闸机通过碰一碰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。具体为：

①每次均需校验是否开通免密支付。

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。

2、离线验证模式下，对闸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。

### 数字人民币硬钱包过闸在线验证模式

1、在线验证模式下，数字人民币硬钱包进站时须进行资金锁定。ITP完成用户鉴权后，向受理银行机构发起资金锁定申请，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。

2、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。

3、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。满足一下要求：

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。

4、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。

# 数字人民币业务应用于AFC专用设备的要求

## 基本要求

Ø参数处理

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。

Ø业务处理

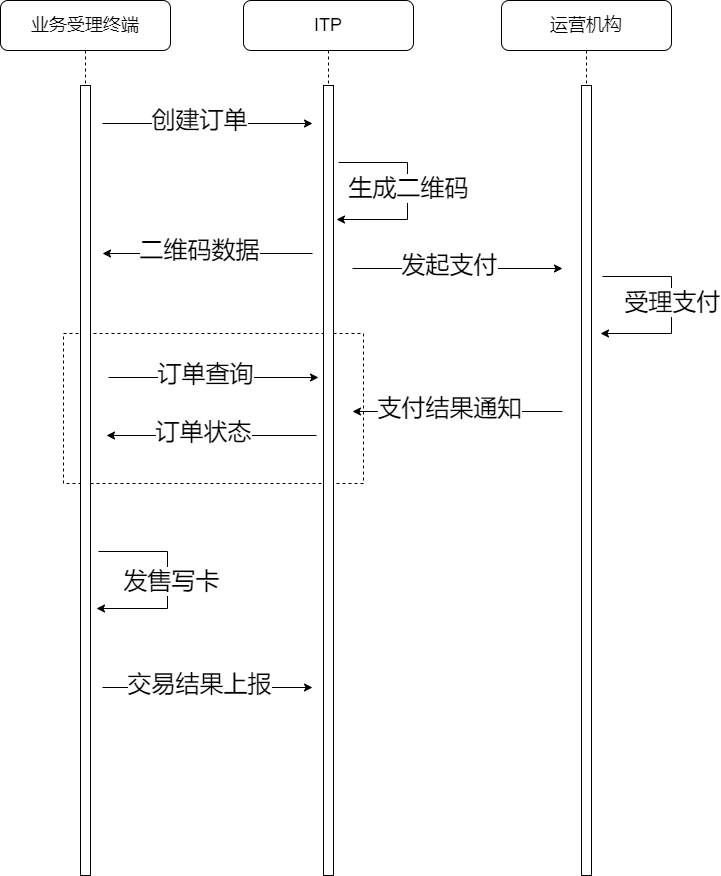
根据数字人民币业务处理流程规范，实现数字人民币支付、查询、补票、退款、进出站等业务处理。

Ø接口处理

实现数字人民币业务与AFC上位系统以及ITP系统的通信及数据接口要求。

## 数字人民币业务在支付场景于专用设备的要求

### 购票模式



1、业务受理终端应向ITP发起订单创建请求，并向用户展示付款码；

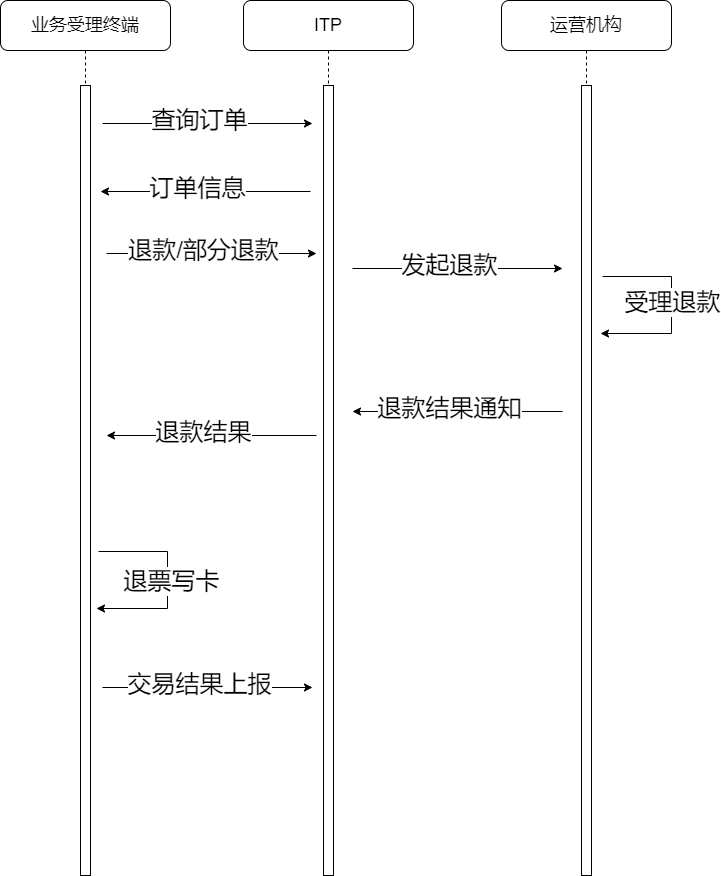
2、业务受理终端应向ITP轮询发起订单状态查询请求，检查订单是否已被支付；

3、当用户支付成功后，ITP应改变订单支付状态。

4、业务受理终端查询到订单已支付后，应执行票卡发售子流程。

5、业务受理终端发售成功后，应向ITP发送发售结果请求。

### 退票模式

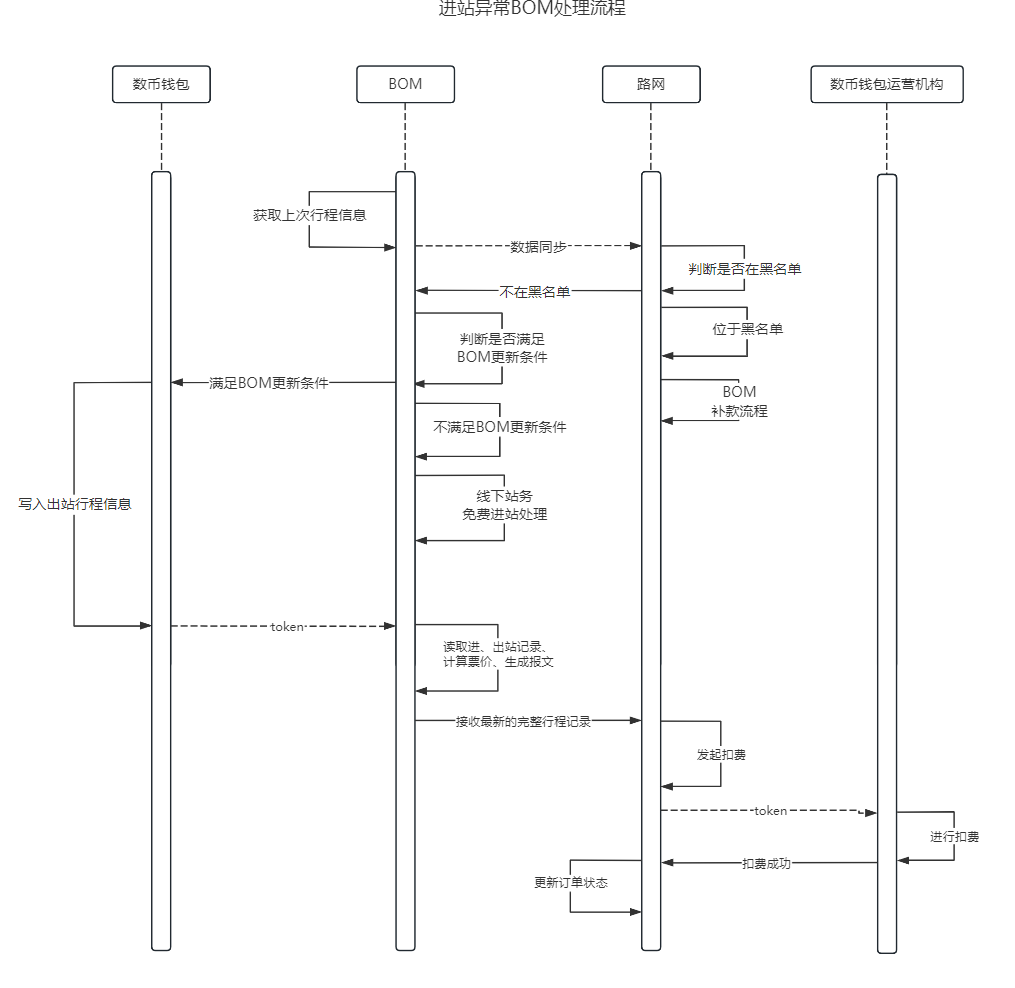


1、业务受理终端应向ITP发送订单查询请求，查询关联支付订单；

2、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发起退款请求；

3、成功后，业务受理终端应完成票卡的退票写卡子流程。

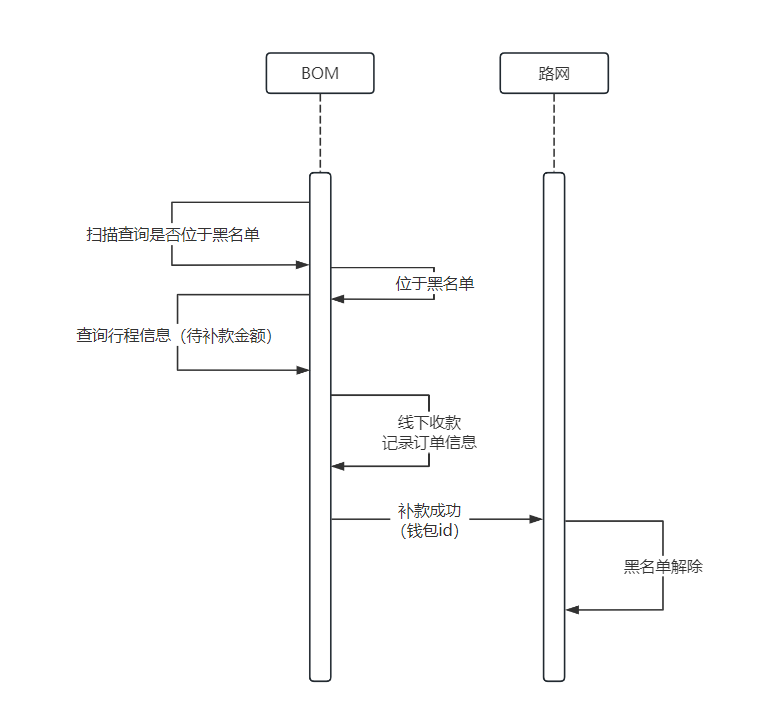
### 进站异常BOM处理流程



1、通过站务BOM系统查询行程信息，判断进站行程的时间，如果是刚刚发生的，那么通过手动方式让用户从边门进入，该处理不在流程体现；如果发生时间过期，那么需要通过BOM完成出站和费用计算、扣费处理。

2、如果在黑名单中，那么通过BOM完成账务处理：如果用户通过现金或其他支付方式完成补款，那么通过BOM更新扣费订单状态为成功，将用户移出黑名单。

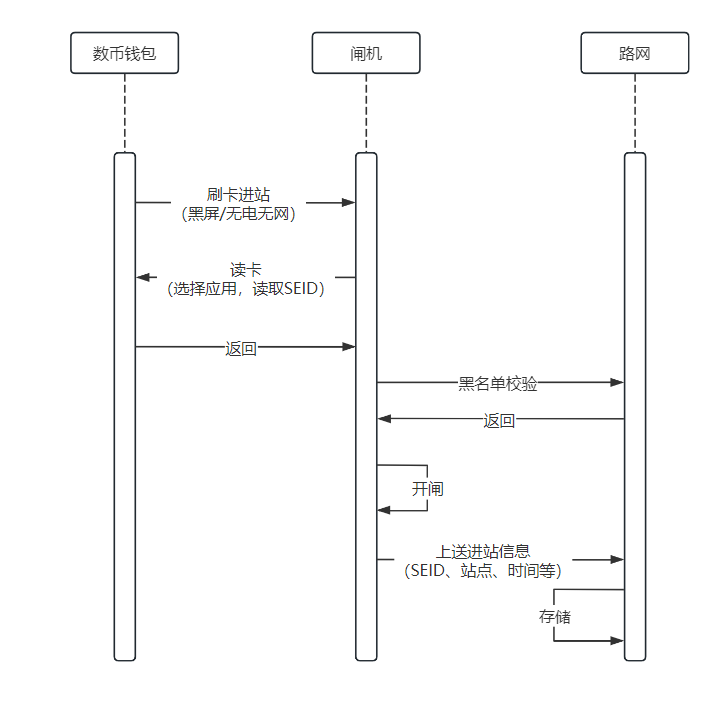
### BOM补款处理流程



支持现金、其他支付渠道扫码，按照数币钱包受理银行补款充值接口原路补款。

## 数字人民币业务在过闸场景于专用设备的要求

### 进站流程



1、用户使用硬钱包，进站时在闸机上碰一碰，通过双向认证校验硬钱包有效性；

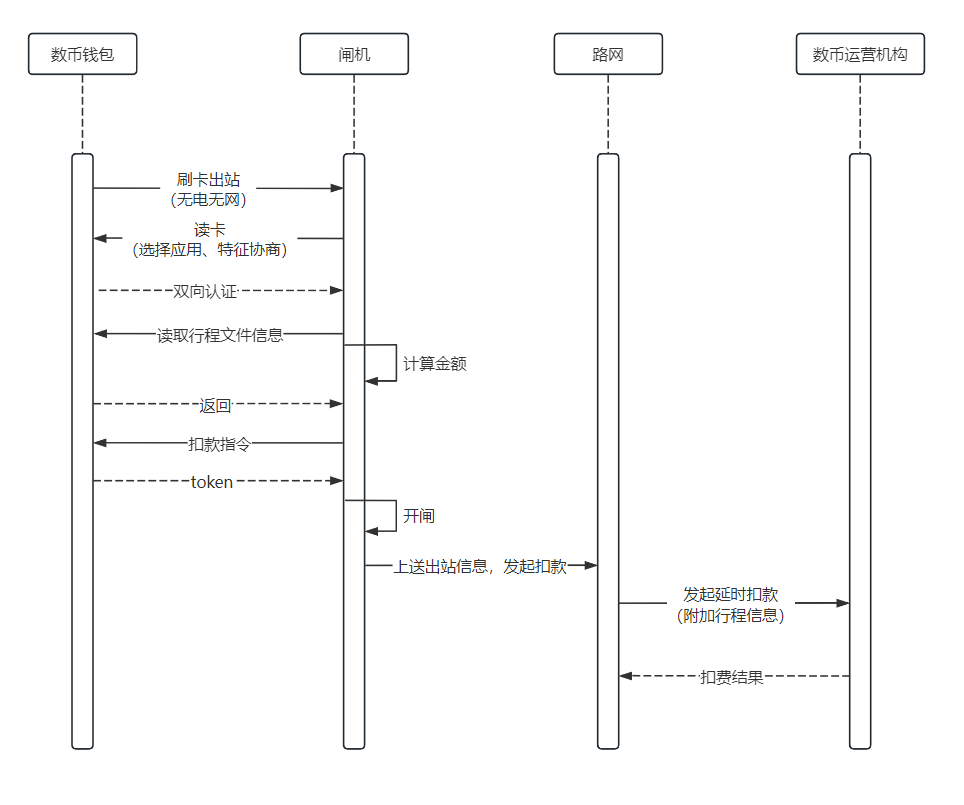
2、闸机读取硬钱包行业应用文件（或连接ITP在线验证有效性），判断行程信息是否正常，若不正常需至BOM处理；

3、闸机调用路网系统完成黑名单校验，若在黑名单中需至BOM处理；

4、黑名单校验通过后开闸，开闸后用户进入车站付费区；

5、闸机传输进站信息给路网系统，路网系统进行存储。

### 出站流程



1、用户使用硬钱包，出站时在闸机上碰一碰，通过双向认证校验硬钱包有效性；

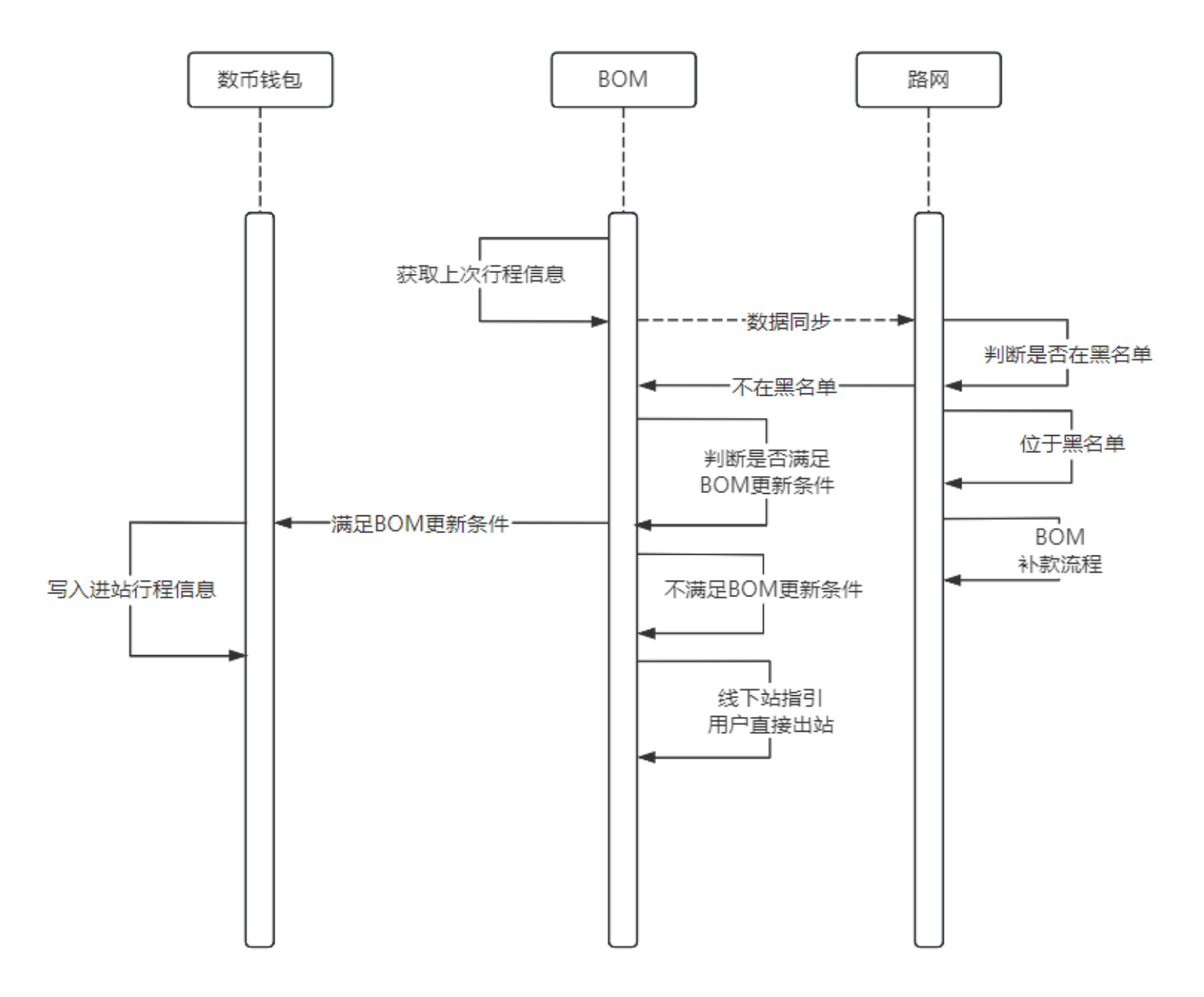
2、闸机读取硬钱包行业应用文件（或连接ITP在线验证有效性），判断行程信息是否正常，若不正常需至BOM处理；

3、闸机根据行程信息，计算费用；

4、闸机调用硬钱包扣款指令，获取钱包生成的扣款token；

5、闸机将出站行程、扣款token信息传输给路网系统。

### 出站异常补行程处理流程



1、通过BOM完成数币硬钱包进站信息补足。

2、补进站后，乘客持数币硬钱包与闸机碰一碰出站，按照正常扣费流程扣费。

## 接口要求

### 与SC系统接口要求

满足SC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。

### 与ITP系统接口要求

满足ITP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。

## 性能要求

数币硬钱包处理速度：≤0.3秒/张（包括识别、校验、编码等）；

从检查数币硬钱包有效后，闸门完全打开时间≤0.3秒；

通信正常的情况下设备的数字人民币数据能在3秒内上传到车站计算机（SC）；

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

# 数字人民币业务在AFC通用读写器的要求

## 总体要求

### 基本要求

1，读写器所使用IC芯片、操作系统满足国产化要求，确保信息安全。

2，读写器的处理器至少满足2核1.5GHZ的工作频率，内存2GB，硬盘8GB容量需求。

3， 读写器能对满足符合PBOC3.0标准（《中国金融集成电路IC卡规范》）和ISO/IEC14443（1-4） TYPE A/B标准的数字人民币硬钱包进行操作。

4，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。

5，读写器实现数字人民币硬钱包的业务处理和业务功能。

6，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；

### 大读写器模式

数字人民币通用读写器应采用大读写器模式：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币硬钱包数据，并进行运营业务处理。读写器根据处理结果进行写卡操作或者与上位设备进行数据交互处理，并组织保存交易记录，在空闲时间将运营记录发送至上位机进行保存处理。大读写器模式提高了数币硬钱包处理速度，同时便于系统的升级改造，提高了数据安全性。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）、自助票务处理机（STM）、移动票务终端（MST）、便携式检验票机（PCA）等AFC专用设备。

### 二维码读头连接方式

设备二维码模块直接与工控机物理连接，由工控机完成二维码数据获取、认证、订单生成和设备动作控制等功能，以实现数币软钱包二维码小额支付业务的处理流程。

## 数字人民币业务支付场景于读写器的要求

售补类设备（如TVM、BOM等)设立于车站非付费区，乘客可以通过数币软钱包进行购票、充值、补票和退款等操作。售补票类设备通过连接于工控机的二维码读头对数字人民币软钱包二维码进行小额支付操作，并通过读写器对符合发售、充值和补票条件的票卡进行读写操作，数币软钱包小额支付交易由读写器统一生成，并按照AFC系统读写器接口标准上传上位系统。

## 数字人民币业务过闸场景于读写器的要求

### 一般功能

数字人民币通用读写器应实现数字人民币硬钱包的识别，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。

### 数币硬钱包在线验证检票流程

#### 进站流程

1.读写器向ITP平台获取收款钱包关联码并储存到读写器闪存（开机只获取一次）。

2.读写器读取收款钱包关联码，判断交易关联码是否存在，若不存在，则不支持此银行机构数币业务。

3.读写器读取数币卡硬钱包信息，根据票价政策设置预授权额度，并执行预授权操作，输出交易凭证：付款token和卡唯一号，保存进站交易记录（进站交易类型、交易时间、终端号、交易流水号、逃票金额、线路编号、站点编号、付款token，卡唯一号和商户订单号等）。

4.上传进站交易到ITP平台。

5.通知检票机开闸放行。

#### 出站流程

1.读写器读取数币卡硬钱包唯一号，并向票务平台联机查询进站交易记录。

2.如果没找到匹配的进站交易记录，则不允许出站；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和卡唯一号；保存出站交易记录（出站交易类型、交易时间、终端号、交易流水号、线路编号、站点编号、付款token，卡唯一号和商户订单号等）。

3.通知检票机开闸放行。

#### 异常处理流程

异常状况指乘客在使用数字人民币硬钱包在线认证模式进出站检票时，遇到的异常情况导致不能正常进出站时，需要通过自助终端或半自动售票机进行异常处理。处理流程如下：

1.读写器读取数币卡硬钱包唯一号，然后查询行程信息，分析异常原因；

2.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。

3.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（进站交易类型、交易时间、终端号、交易流水号、逃票金额、线路编号、站点编号、付款token，卡唯一号和商户订单号等）。然后正常刷卡出站。

### 数币硬钱包离线验证检票流程

（1）乘客需要提前开通包含乘客行程文件区的数币硬钱包；

（2）读写器内需要安装数字人民币PSAM卡，PSAM具备本地扣费及更新行程文件的能力，且能满足各地轨道交通相关标准要求。

#### 进站流程

（1）乘客进站时，读写器读取数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。

（2）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（进站交易类型、交易时间、终端号、交易流水号、逃票金额、线路编号、站点编号、付款token，卡唯一号和商户订单号等）。

（3）通过检票机上传进站交易到票务平台。

（4）通知检票机开闸放行。

#### 出站流程

（1）乘客出站时，读写器读取数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和卡唯一号。

（2）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（进站交易类型、交易时间、终端号、交易流水号、逃票金额、线路编号、站点编号、付款token，卡唯一号和商户订单号等）；

（3）通过检票机上传出站交易到票务平台；

（4）通知检票机开闸放行。

#### 异常处理流程

异常状况是指乘客在使用数字人民币硬钱包离线认证模式进出站检票时，遇到的异常情况导致不能正常进出站时，需要通过自助终端或半自动售票机进行异常处理。业务流程如下：

1、读写器读取数币卡硬钱包行程信息，然后分析异常原因；

2、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，形成补款交易记录（补缴交易类型、交易时间、终端号、交易流水号、线路编号、站点编号、付款token，卡唯一号和商户订单号等）；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。

（4）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（进站交易类型、交易时间、终端号、交易流水号、逃票金额、线路编号、站点编号、付款token，卡唯一号和商户订单号等）；乘客重新刷卡出站。

## 与ITP接口要求

（1）商户钱包关联码查询，请求参数和响应参数。

（2）预授权接口，请求参数和响应参数。

（3）预授权完成接口，请求参数和响应参数。

（4）数币进站与出站匹配接口，请求参数和响应参数。

## 技术指标

1、RF射频部分技术指标符合ISO/IEC14443（1-4） TYPE A/B标准

2、安全认证模块部分技术指标：

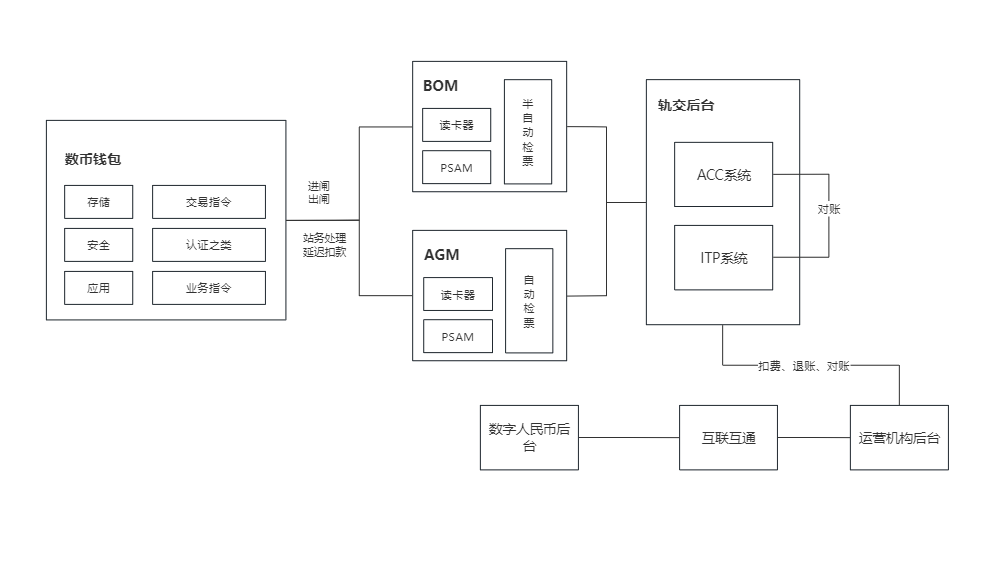
SAM卡插座符合GSM11.11标准。

SAM卡接口符合ISO/IEC7816-1、2、3、4技术标准。

3、读写时间

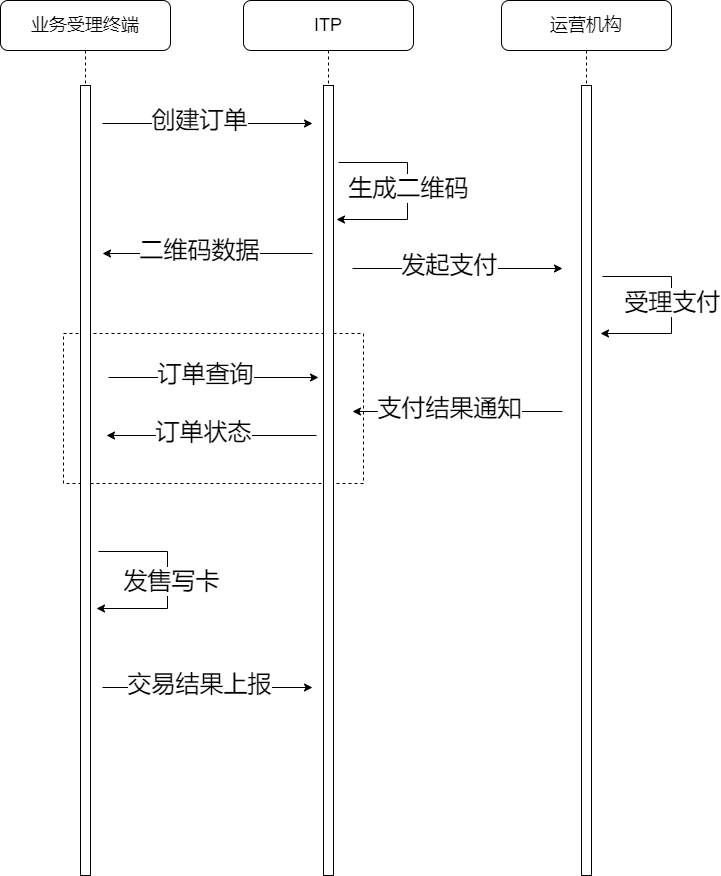
|  |  |
| --- | --- |
| 车票类型 | 检票机进出读写时间 |
| 轨道交通专用票 | 200 ms |
| 储值票（标准卡） | 400 ms |
| 数字人民币硬钱包卡 | 300 ms |
| 注：读写时间指从捕获到卡至卡交易过程数据读写全部结束的过程，包含读写过程中ECU端的处理时间；不包含交易记录的产生及设备开门、出票等动作。 | |

# 数字人民币业务AFC应用软件要求



## 数字人民币业务支付场景的应用软件要求

### 购票流程



1、业务受理终端应向ITP发起订单创建请求，并向用户展示付款码；

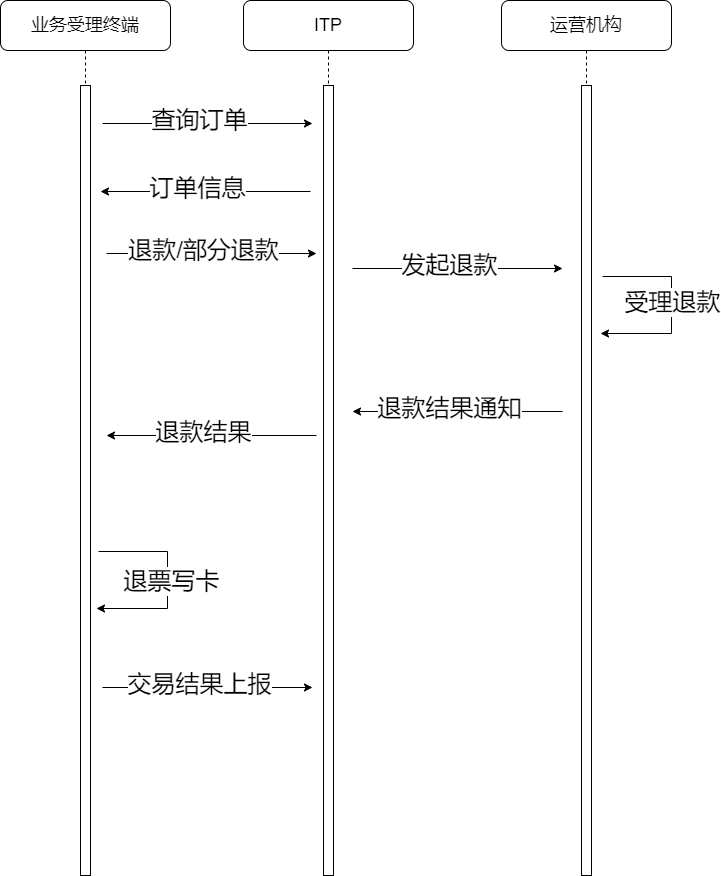
2、业务受理终端应向ITP轮询发起订单状态查询请求，检查订单是否已被支付；

3、当用户支付成功后，ITP应改变订单支付状态；

4、业务受理终端查询到订单已支付后，应执行票卡发售子流程；

5、业务受理终端发售成功后，应向ITP发送发售结果请求。

### 退票流程

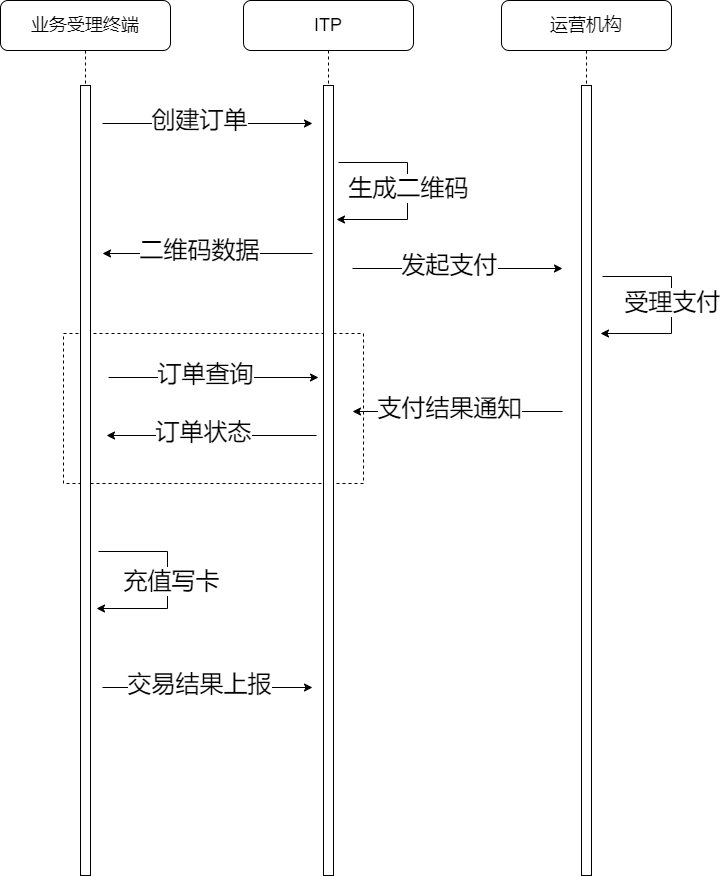


1、业务受理终端应向ITP发送订单查询请求，查询关联支付订单；

2、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发起退款请求；

3、成功后，业务受理终端应完成票卡的退票写卡子流程。

### 充值流程



1、业务受理终端应向ITP发起订单创建请求，并向用户展示付款码；

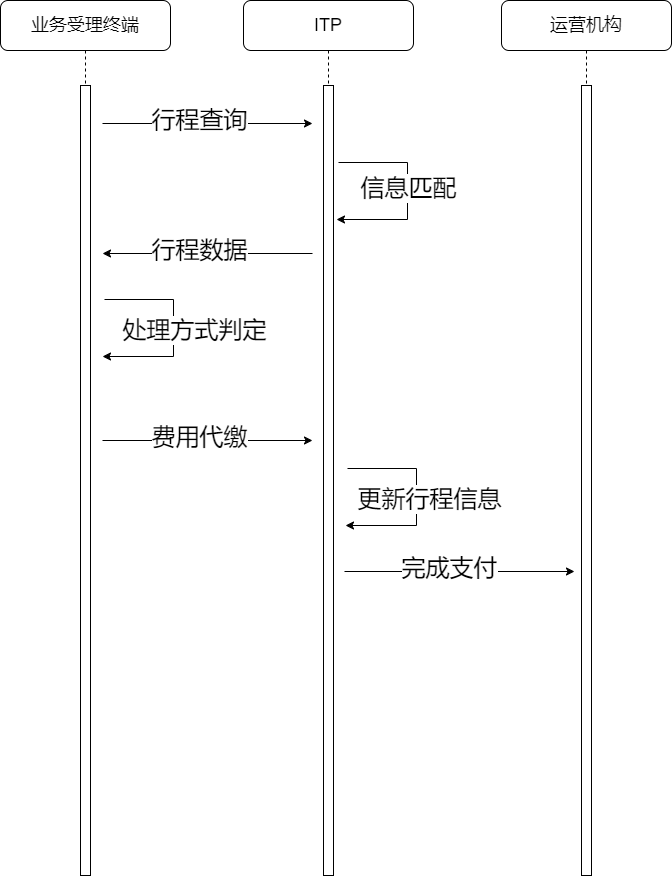
2、业务受理终端应向ITP轮询发起订单状态查询请求，检查订单是否已被支付；

3、当用户支付成功后，ITP应改变订单支付状态；

4、业务受理终端查询到订单已支付后，应执行票卡充值写卡子流程；

5、业务受理终端充值票卡成功后，应向ITP发送充值结果请求。

### 费用补缴流程



1、业务受理终端查询到待缴费行程后，应提示乘客补缴行程费用；

2、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。

### 异常处理流程

1、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；

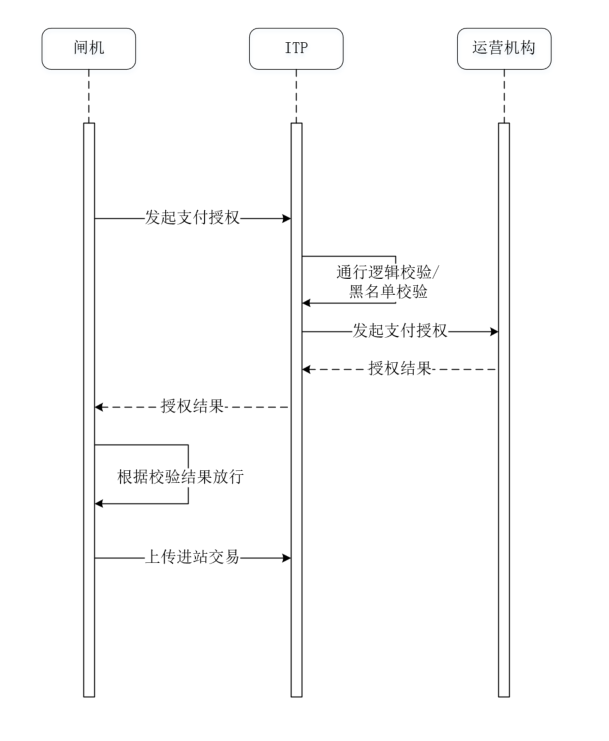
2、业务受理终端应根据订单号向互联网业务平台发起退款或部分退款请求；

3、若成功后，业务受理终端应保存相关交易信息；

4、若失败，业务受理终端应提示失败信息或进行定时重试子流程。

## 数字人民币业务过闸场景的应用软件要求

### 进站流程



1、闸机应按线网规程规定票价向ITP发起支付授权请求；

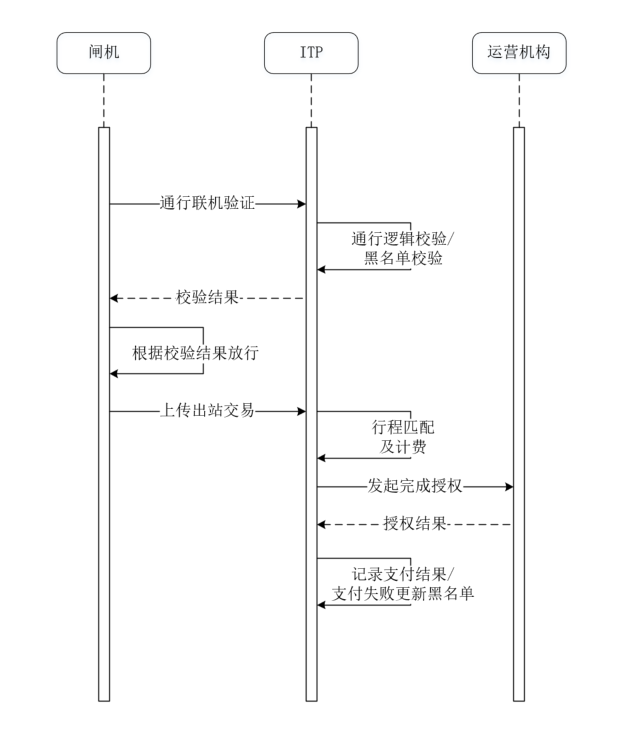
2、ITP应根据业务规则进行通行逻辑校验（行程OD状态等）、黑名单校验；

3、校验通过后，ITP应向运营机构发起支付授权请求；

4、闸机应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、闸机应实时向ITP上传进站交易。

### 出站流程



1、闸机应向ITP发起出站通行联机验证请求；

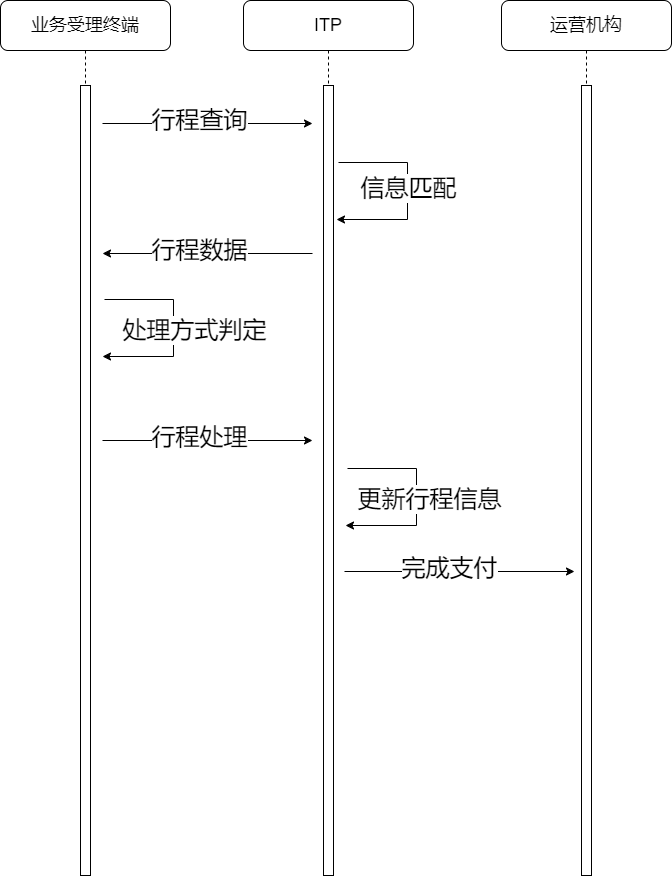
2、ITP应根据业务规则进行通行逻辑校验（行程OD状态等）、黑名单校验；

3、闸机应根据ITP的校验结果进行开闸放行，并向ITP上传出站交易；

4、ITP应根据进站交易和出站交易进行行程匹配及计费；

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。

### 行程更新流程



1、业务受理终端应向ITP发起行程查询请求；

2、业务受理终端收到行程信息后，应根据轨道交通相关票务规则，判定其更新方式，并展示给用户；

3、业务受理终端应根据用户选择，并向ITP发起行程处理请求，完成更新操作。

## 接口要求

### 与运营机构机构接口

1、实现钱包授权、支付、退款及结果通知等接口，满足运营机构支付业务处理要求；

2、实现交易对账接口，满足运营机构对账单业务处理要求。

### 与终端设备接口

1、终端设备订单创建、查询、授权、验证等接口，满足AFC系统定义的数字人民币钱包业务处理要求。

2、满足数字人民币在AFC线网中的业务风控需求。

3、与清分中心接口，满足运营机构支付账单与AFC交易的对账及清结算要求。

## 性能要求

### 并发处理

1、过闸业务整体通行时间<=1000ms；

2、平台并发数满足系统内所有设备同时在线连接请求要求；

3、交易数据处理能力满足运营日系统设计要求。

### 软件系统扩展性要求

1、满足用户需求管理且满足需求变化及扩展需要

2、满足可适应运营规则变化的功能扩展需要

3、满足系统各组成软件模块的增加、变更及组合的应用需要

4、满足低成本且可便捷实现系统功能的变化及扩展需要

5、满足轨道交通其它关联应用的扩展需要

6、系统设计时须做好技术预留，具备兼容其他第三方APP实现数字人民币支付条件

## 软件系统安全性要求

1、软件系统应具有操作权限管理功能

2、利用所有在系统内的操作和交易记录，可进行完整的审计追踪

3、软件系统自身应具有自监测、自诊断和充分的冗余功能。第三方软件（如防病毒软件、备份软件等）具有自动运行的能力。

4、软件系统应可防止对数据的恶意破坏

5、软件系统应具有防止误操作及恶意操作的功能

6、软件系统的更新应保证安全、有序且不影响正常运营

# 数字人民币业务系统对运行环境及性能的要求

## 可靠性要求

关键设备、系统需进行冗余配备，应用系统支持集群模式。

系统可 7\*24 小时不间断稳定运行，不存在单点风险。

平均无故障时间指标 MTBF 不低于 100,000 小时。

平均故障修复时间指标 MTTR 不高于 15 分钟。

## 安全性要求

针对数字人民币小额支付以及进出站过闸业务的应用，建立多层次安全防护体系。

### 账户信息安全

账户信息存储需符合相关信息安全法律法规及要求。

### 数字人民币信息安全

需在数据解析过程中对数字人民币数据信息的完整性、真实性、不可抵赖性及时效性进行鉴别，对于未通过鉴别等非法数字人民币支付码将予以阻止。

### 传输安全

需在系统内以及与其他系统之间将建立安全通信通道，对交易数据采用数字签名和加密等安全方式进行传输，确保数据不被监听和篡改。业务受理终端与平台之间的交易报文应实现签名、并在通信时进行验签；涉及用户隐私的信息需在传输时加密。

### 数据安全

应采用电子安全交易手段，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，应符合国际、国家和建设部、中国人民银行等行业技术标准及规范中有关交易安全的要求。

### 系统安全

系统应采取关键计算、网络、安全设备冗余措施，对整个系统进行配置、监视和管理。能够有效识别出系统中存在的病毒危害、非法操作、异常事件和外部攻击等威胁，并通过边界隔离、内部监测审计和主机防护，为AFC系统提供全方位的综合防御与保护。

### 数据存储安全

应保障用户公私钥、机构授权等信息的安全，采用敏感数据分段存储，且智能终端客户端程序应保证分段数据组合过程编程逻辑的安全性。应禁止在身份认证结束后明文存储账户信息，防止账户信息泄露。支付交易中涉及敏感数据离线存储需要进行安全保护，例如：用户数币钱包关联码等。

## 扩展性要求

运行环境需要具备较强的计算和存储能力，以确保系统能够高效处理大规模的交易数据；能够根据实际需求灵活调整系统资源配置，确保系统能够应对高峰期的交易压力，具备良好的横向扩展能力，能够方便地添加新的功能与服务。

## 可维护性要求

需提供良好的配置管理工具和升级机制，确保可以轻松的配置和管理各种组件和服务，快速、安全的进行升级和更新。需建立完善的监控和管理体系，实时监测基础设施和平台服务系统的运行状态和性能，及时发现和解决问题。

## 兼容性要求

需与AFC系统的其他组件和设备兼容，确保数字人民币业务能够与现有系统集成。

## 合规性要求

需符合金融监管和相关法律法规及要求。

## 接口要求

1，对内接口

需满足对数字人民币参数、交易数据等数据传输的支持。

2，对外接口

需满足对数字人民币业务相关签约、支付、查询等接口的支持。