Q/CUP

中 国 银 联 股 份 有 限 公 司 企 业 标 准

Q/CUP 007.4.4—2014

银联卡受理终端安全规范
第 4 卷：辅助卷
第 4 部分：基于地理位置定位的终端非法移机监控技术方案

Security Specifications for Terminal Accepting UnionPay Card
Volume 4: Auxiliary Requirements
Part 4: Technical Scheme of Monitoring Terminal Illegal Moving based on Geographical Location

2014-11-30 发布　　2014-12-01 实施

中国银联股份有限公司 发布

目　　次

前　言

本标准对受理银联卡（包括磁条卡和IC卡）终端的硬件和安全做具体规定。

本标准由以下部分组成：

——第1卷：基础卷

——第1部分：术语

——第2部分：设备安全

——第3部分：管理安全

——第4部分：硬件要求

——第2卷：产品卷

——第1部分：销售点（POS）终端

——第2部分：无人值守（自助）终端

——第3部分：个人支付终端

——第4部分：独立部件

——第5部分：电话终端

——第6部分：智能销售点终端

——第7部分：mPOS通用技术安全

——第3卷：检测卷

——第1部分：基础安全检测要求

——第2部分：产品分类安全检测要求

——第3部分：硬件技术检测要求

——第4卷：辅助卷

——第1部分：终端防切转网技术安全指南

——第2部分：航空机上支付技术安全指南

——第3部分：POS互联网接入系统部署方案

——第4部分：基于地理位置定位的终端非法移机监控技术方案

本部分为《银联卡受理终端安全规范》第4卷第4部分。

本部分由中国银联提出。

本部分由中国银联技术部组织制定和修订。

本部分的主要起草单位：中国银联、福建联迪商用设备有限公司、百富计算机技术有限公司、深圳新国都技术股份有限公司、福建新大陆电脑股份有限公司、福建升腾资讯有限公司、银行卡检测中心。

本部分的主要起草人：吴潇、夏庆凡、倪国荣、陈瑞兵、杨超杰、张正伟、李洲明、刘祥洪、方丰、余杭军、张贵潭、安焘。

银联卡受理终端安全规范
第 4 卷：辅助卷
第 4 部分：基于地理位置定位的终端非法移机监控技术方案

1 范围

经前期对终端市场的调研来看，未来几年内，商户对移动POS终端和互联网POS终端的需求量将急剧增长。而近年来，终端市场上存在不法分子为规避信用卡套现检查，将POS终端挪到隐蔽场所进行非法套现，或将低扣率（例如批发市场）终端挪到高扣率（例如宾馆酒店）商户使用的情况。中国人民银行为加强银行卡业务管理，维护银行卡市场秩序，于2014年初发文要求收单机构规范银行卡受理终端的使用，严格控制移动POS终端的布放范围。为缓解市场需求与监管层面的矛盾，特编制《监控POS终端非法移机的解决方案》，针对市场上的金融POS终端（包括移动POS、拨号POS、以太网POS、mPOS等）提出监控其非法移机的解决方案，提供移机风险识别及预警，供事后进行人工核查。

2 规范性引用文件

下列文件中的条款通过本标准的引用而成为本标准的条款。凡标注日期的引用文件，对于标注日期之后所有的修改单（不包括勘误的内容）或修订版均不适用于本标准，但是，鼓励根据本标准达成协议的各方研究是否可使用这些引用文件的最新版本。凡不标注日期的引用文件，其最新版本均适用于本标准。

3 方案一：POS 终端和移动基站绑定方案

3.1 终端类型

适用于各类移动终端、台式终端。

3.2 硬件要求

必须具备2G/3G/4G通讯模块，该模块需具备收集基站信息功能。

3.3 具体方案

3.3.1 模糊定位

1、终端初装时通过通讯模块采集基站信息列表，并上送到后台，保存为终端位置信息基值；

2、后续终端在每次交易时采集当前基站信息列表上送后台；

3、后台将其与位置信息基值进行比较，若无相同基站信息则认为该终端发生移机风险并告警。

3.3.2 精确定位

1、终端初装时通过通讯模块采集基站信息列表，并上送到后台，后台通过LBS系统得到经纬度信息，保存为终端位置信息基值；

2、后续终端在每次交易时采集当前基站信息列表上送后台；

3、后台依然通过LBS系统得到该交易的经纬度信息及详细地址信息，并与位置信息基值经纬度计算出位置距离，当距离大于某个值时则认为该终端发生移机风险并告警，同时告警系统显示移机发生详细地址信息及报备的终端布放地址，方便人工风险核查。

3.3.3 方案比较

——模糊定位方案不依赖于LBS系统，实施成本相对比较低；但由于基站信息变动或搜索不全可能引起移机误判；只能判断终端是否被大范围的移动，且无法确定其具体地址；定位的准确性受基站密度影响较大。

——精确定位方案投入成本高，后台实施周期长，但可以较准确的判断终端的移动范围。

3.4 终端改造需求

——对已包含2G/3G/4G通讯模块的终端，需对软件改造以支持基站信息采集及上送后台；

——对不具备该通讯模块的终端(如传统拨号终端、以太网终端)，建议硬件升级增加2G/3G/4G模块，然后软件改造支持基站信息采集及上送后台。

3.5 平台改造需求

——对于模糊定位，平台需保存终端位置信息基值，交易受理时进行基站信息列表比对，并进行移机风险识别并预警；

——对于精确定位，需连接LBS系统（可自建或购买服务），平台与该系统交互完成基站地址信息与经纬度值和详细地址信息的转换；平台需保存终端位置信息经纬度基值，交易受理时与位置信息基值计算位置距离并判断，完成移机风险识别并预警。

3.6 规范的修订需求

以GSM网络为例，交易报文建议增加如下字段：

字段名称	字段类型与长度	字段描述	条件
MCC	Varchar(3)	移动国家代码	可选
MNC	Varchar(1)	移动网络号码	必选
LAC	Varchar(4)	位置区域码	必选
CID	Varchar(4)	基站编号	必选

建议使用报文域：域62。

3.7 业务或风险上的补充

收单机构应至少对终端布放地址进行后台远程确认或现场布放确认，业务上规定终端初装时需现场采集终端位置信息基值或后台根据交易上送的位置信息设置正确的终端位置信息基值。

4 方案二：利用电信运营商的定位服务对终端进行定位的方案

4.1 终端类型

适用于各类移动终端。

4.2 硬件要求

——应具备 2G/3G/4G 通讯模块；

——应插入 SIM 卡。

4.3 具体方案

1、终端初装时获取SIM卡的IMSI号并上报给后台，后台通过调用电信运营商的接口获取终端当前的地址信息，保存为终端位置信息基值；

2、后续每次交易终端获取SIM卡的IMSI号并上报后台，后台首先检查IMSI是否发生变化，并通过调用电信运营商的接口获取终端当前的地址信息，并与位置信息基值相比计算出是否有差异；

3、当IMSI号发生变化或位置发生较大差异时，则认为该终端发生移机风险并告警，同时告警系统显示移机发生详细地址信息及报备的终端布放地址，方便人工风险核查。

4.4 终端改造需求

需对软件改造以支持IMSI上送后台。

4.5 平台改造需求

——终端初装时，将上送的SIM卡IMSI信息发送给电信运营商，得到终端当前地址信息，并保存为终端位置信息基值；

——把交易信息中SIM卡的IMSI信息，发送给电信运营商，并得到终端当前的位置信息；

——比较交易时终端位置信息与终端位置信息基值是否发生变化；

——需将终端与IMSI进行绑定，后续用于判断IMSI是否发生变化；

——当IMSI号发生变化或位置发生较大差异时，则认为该终端发生移机风险并告警，同时告警系统显示移机发生详细地址信息及报备的终端布放地址，方便人工风险核查。

4.6 规范的修订需求

交易报文建议添加如下字段：

字段名称	字段类型与长度	字段描述
IMSI	Varchar(15)	国际移动用户识别码

建议使用报文域：域62。

4.7 业务或风险上的补充

——后台需将SIM与终端进行绑定；

——收单机构应对终端布放地址进行后台远程确认或现场布放确认，业务上规定终端初装时需现场采集终端位置信息基值或后台根据交易上送的位置信息设置正确的终端位置信息基值。

5 方案三：通过智能手持设备获取位置信息定位 mPOS 终端的方案

5.1 终端类型

仅适用于mPOS。

5.2 软件要求

——上位机应提供可靠的位置服务，包括GPS、A-GPS、WIFI等；

——支付应用软件应可识别出上位机是否人为关闭位置服务，如关闭则提醒打开，否则不允许交易；

——支付应用软件应能根据不同的移动网络制式（GSM/CDMA/WCDMA/WLAN等）获取当前的位置信息，并且随交易报文一同上送后台；

——支付应用软件应使用经纬度信息；

——为避免对客户体验造成影响，终端位置信息可采用定期获取的方式。例如，支付应用软件在登录时获得当前位置信息，并定期（如10分钟）更新一次，保存在内存中，在交易报文中上送。

5.3 具体方案

1、终端初装时通过支付应用软件采集终端位置信息，并上送到后台，保存为终端位置信息基值；

2、后续每次交易时上送当前位置信息至后台；

3、后台将其与位置信息基值进行比较，若位置发生较大差异，则认为该终端发生移机风险并告警，同时告警系统显示移机发生详细地址信息及报备的终端布放地址，方便人工风险核查。

5.4 规范修订需求

交易报文建议增加如下字段：

字段名称	字段类型与长度	字段描述	条件
Longitude	Varchar(8)	经度	必选
Latitude	Varchar(8)	纬度	必选

建议使用报文域：域62。

5.5 平台改造需求

——应能存储交易相对应的位置信息；

——终端开通时应保存位置信息基值，用于移机判断标识；

——可通过人工输入方式预设终端布放位置信息基值；

——交易发生时，根据位置监控要求能够进行终端移机的告警；

——通过对交易的位置信息分析，定期产生移机风险报表，供收单机构进行风险防控；

——平台能够接收和识别当前经纬度信息并用于移机监控。

5.6 业务或风险上的补充

——针对本方案应加强风险管理级别；

——收单机构应对终端布放地址进行后台远程确认或现场布放确认，业务上规定终端初装时需现场采集终端位置信息基值或后台根据交易上送的位置信息设置正确的终端位置信息基值。

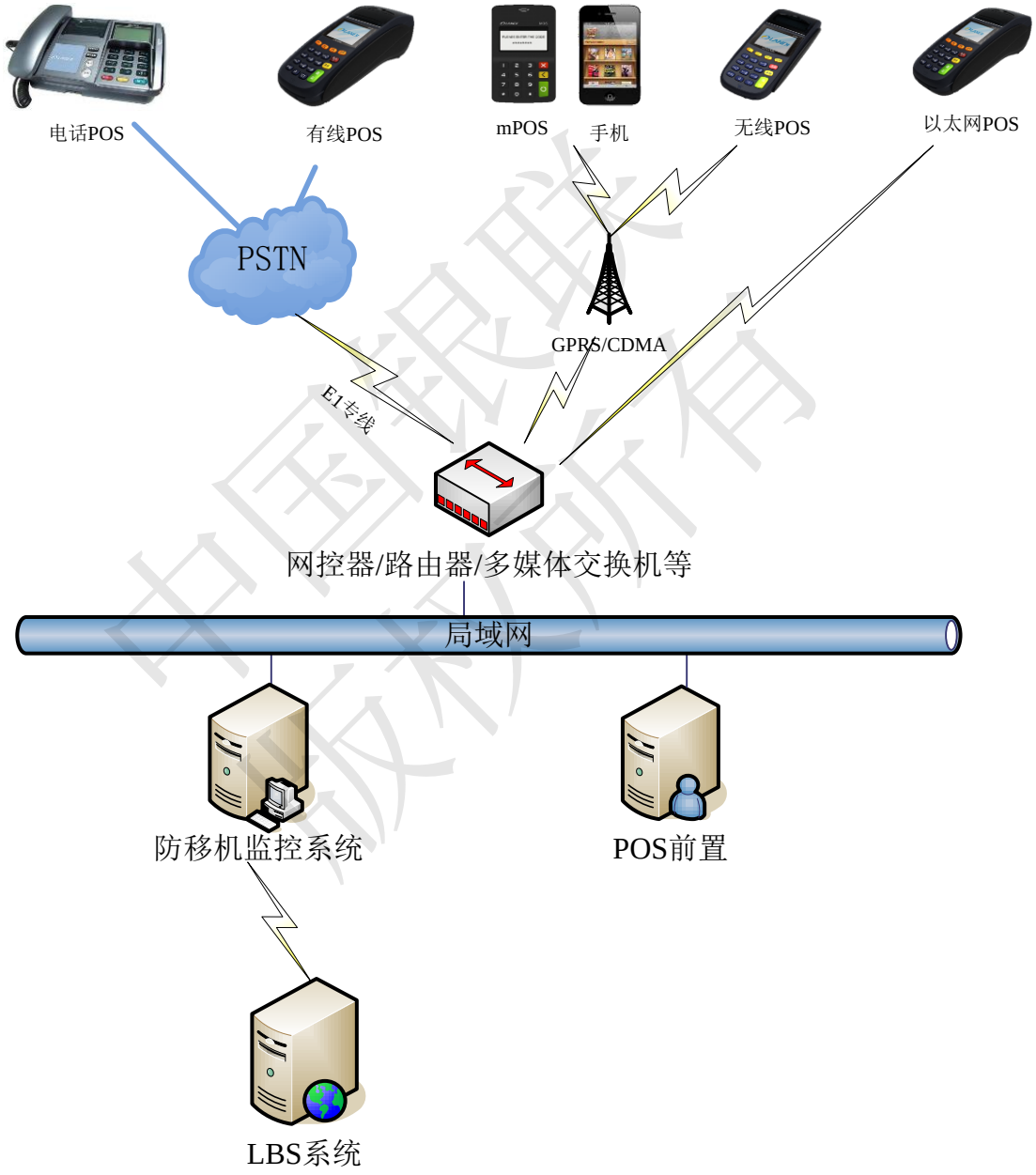
6 方案特点分析

方案	适用范围	成本投入	定位精度	终端改造量	可行性
方案一：POS终端和移动基站绑定方案	移动POS、台式POS	模糊定位：较低 精确定位：较高	模糊定位：中 精确定位：高	硬件需具备无线通讯模块；同时需对软件进行相应改造	模糊定位：高 精确定位：中
方案二：利用电信运营商的定位服务对终端进行定位的方案	移动POS	较高	高	硬件需具备无线通讯模块；同时需对软件进行相应改造	中。 可与方案一中的模糊定位相结合，用于对移机风险较大的终端进行事后分析。
方案三：通过智能手持设备获取位置信息定位mPOS终端的方案	mPOS	较低	高	需对支付应用软件进行改造	高

说明：对收单业务而言，手机和平板是相对不安全的设备，位置信息可能被非法应用篡改，因此需配合业务和风险方面的管控手段，加大管控力度。

7 防移机监控系统建设需求

7.1 系统结构图



7.2 业务流程

7.2.1 基准位置采集

收单机构在给商户安装POS时，利用POS采集该终端被允许移动使用范围的中心位置(我们称之为基准位置)的若干基站信息(包括LAC、CellId、Mnc、Mcc等)，并设置允许偏差距离，上送POS前置，POS前置分解出基站信息并转发到防移机监控系统，防移机监控系统将基准位置的若干基站信息及允许偏差距离保存到数据库中。

7.2.2 交易位置上送

商户使用POS进行交易时，POS采集交易位置附近的若干基站信息，随同交易信息一起上送POS前置，POS前置分解出基站信息并转发到防移机监控系统。

7.2.3 移机监控处理

根据终端的使用场景，用户对定位的精度要求，可以选择以下两种监控方案：

——锁小区方案(模糊定位)：防移机监控系统比较该终端基准位置和交易位置的基站信息，看二者之间是否有交集，如果有交集则判定未移机，否则判定已移机，并登记风险记录。

——LBS定位方案(精确定位)：防移机监控系统将该终端的基准位置和交易位置的基站信息送往电信运营商(或拥有基站信息数据的第三方机构)的LBS系统，LBS系统返回这两个位置的经度、维度和具体地理位置，防移机监控系统根据经度、维度计算两位置之间的距离，如果两者之间的距离未超过允许的偏差距离则判定未移机，否则判定已移机，并登记风险记录。

7.2.4 报表生成及查处

防移机监控系统定期生成违规移机终端报表，为收单机构查处提供依据。

7.3 功能要点

7.3.1 系统管理

系统管理主要是对分支机构、权限、操作员、系统参数等进行管理维护。

——机构管理：本系统中各分支机构的数据应相互隔离，可以按总公司、分公司、办事处等对机构进行分级管理，上级可以访问本机构及下属机构的数据，同级之间数据互相隔离，从而保证数据安全。

——权限管理：在系统的实际使用中，一个用户所对应的访问系统的能力是由一个权限组进行控制的，这个就是权限管理。通过权限组设置，可以定义不同的角色，分配不同的功能访问权限。

——操作员管理：本系统在初始化时，创建高级系统用户，并由高级系统管理员对自身的安全密码进行修改而确保系统的安全性，高级系统用户对本系统有全权管理权限，负责整个系统的技术保障工作，可以根据需求定义导入导出的接口，保障系统的扩展性。本功能模块主要实现对用户增加、修改、删除、查询功能。

——参数管理：系统参数管理，例如LBS系统服务器的IP地址、端口号等。

7.3.2 后台服务

——基准位置登记：将终端上送的或手工方式录入的基准位置的基站信息登记到防移机监控系统数据库中。

——移机监控处理：根据终端的基准位置和交易位置的基站信息，判断终端是否超地域范围使用。当发现POS移机使用时，可选择采取以下一种或几种措施加以处理。

- 向收单机构管理人员提供告警信息，提醒收单机构管理人员采取必要措施。
- 实时锁定POS终端，禁止POS交易。
- 定期生成风险终端报表。

——风险交易监控：实时显示疑似移机使用的POS终端交易，显示其地理位置信息(仅限于精确定位方案)，并通知相关管理人员采取措施。监控界面如下所示：

注	收单机构	商户号	终端号	流水号	交易日期	交易时间	交易位置
	123456789012	123456789012345	88880001	000006	2012/10/10	13:14:15	上海市含笑路8号

7.3.3 报表生成

——风险终端汇总报表生成：根据用户输入的时间段、机构号、商户号、终端号等筛选条件，从风险流水表中生成风险终端汇总报表，列明风险发生的商户号、终端号、风险发生次数等。具体格式如下：

点击查看功能，还能在地图上展示这些交易发生的地点。

——风险交易明细报表生成：根据用户输入的时间段、机构号、商户号、终端号等筛选条件，从风险流水表中生成风险交易明细报表，列明风险发生的商户号、终端号、流水号、交易金额、交易日期、交易时间、交易地点等。报表格式如下：

统计起止日期：YYYY 年 MM 月 DD 日- YYYY 年 MM 月 DD 日　　机　构：

报表生成日期：YYYY 年 MM 月 DD 日　　操作员：

商户号	终端号	流水号	交易金额	交易日期	交易时间	交易地点
123456789012345	88888888	112	2000.12	2012/12/1	12:23:40	上海市含笑路 8 号