Q/CUP

中 国 银 联 股 份 有 限 公 司 企 业 标 准

Q/CUP 007.4.3—2014

银联卡受理终端安全规范
第 4 卷：辅助卷
第 3 部分：POS 互联网接入系统部署方案

Security Specifications for Terminal Accepting UnionPay Card
Volume 4: Auxiliary Requirements
Part 3: System Deployment Scheme for Internet Access POS

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3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、银行卡检测中心、福建升腾资讯有限公司、福建联迪商用设备有限公司、百富计算机技术（深圳）有限公司、深圳市新国都技术股份有限公司、福建新大陆支付技术有限公司。

本部分的主要起草人：吴潇、徐燕军、李伟、李洁、谭颖、王建新、张贵潭、胡伟、倪国荣、蒋鹏、杨超杰、彭荣收、黎景阳、陈乐、周红弟。

银联卡受理终端安全规范
第 4 卷：辅助卷
第 3 部分：POS 互联网接入系统部署方案

1 范围

本《方案》对POS以互联网方式接入的系统方案进行举例，作为建议供收单机构和生产企业参考。

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。

银联风管委【2013】9号 银联卡收单机构账户信息安全管理标准

Q/CUP 058 银联卡密码算法使用与密钥管理规范

Q/CUP 007.1 银联卡受理终端安全规范-第1卷-基础卷

3 接入方案一：SSL/TLS 单向认证方案

3.1 概述

本方案适用于终端直接采用SSL/TLS安全通讯协议接入互联网，且实施时选择的是单向认证。单向认证指的是终端对系统平台的认证，确保终端接入合法的系统。

3.2 终端要求

——CA根证书用于校验平台的合法性，其由平台进行生成和分发；终端应在安全环境下注入CA根证书，并确保其合法性，避免任意的CA根证书注入到终端；同时终端应保证CA根证书的安全存储，防止其被非法替换或更新。

——终端应支持存储多个CA根证书，以便终端接入多个平台。

——终端在SSL/TLS交互过程中应严格按照SSL/TLS协议要求，使用CA根证书对平台端的公钥证书进行校验。

3.3 平台要求

——平台系统应安全产生、管理和使用平台证书；

——平台系统应能防止交易重放攻击；

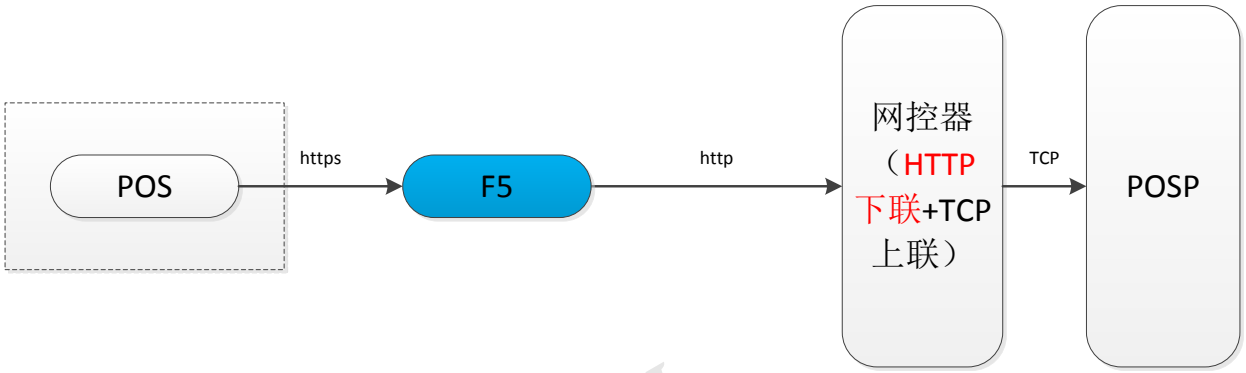
——平台私钥应被安全存储；

——平台应满足互联网环境下支付系统的相关安全管理要求，详见《银联卡收单机构账户信息安全管理标准》（银联风管委【2013】9 号）。

3.4 实施参考

以下实施方案供参考，具体以实际平台状况确定具体的实施方案。

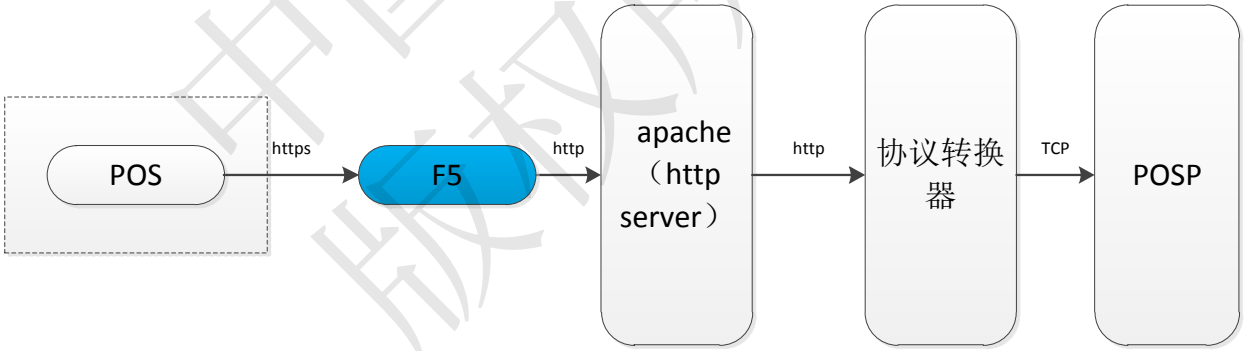
3.4.1 实施参考一



终端采用https单向认证接入互联网，系统平台只需少量开发以及新增设备即可满足POS终端支持互联网接入。具体实施要点如下：

1、 终端开发支持https单向认证，原8583报文或其它报文（例如脚本等）直接通过https进行交互；
2、 终端布放时安全下装CA根证书，https交互时通过CA根证书验证平台合法性；
3、 平台在F5设备上部署平台端证书，实现https单向认证接入以及报文转换，由网络接入控制器设备完成http报文到内部应用接口的转换，网络接入控制器设备需配置http下联卡和TCP/IP上联卡；
4、 POSP平台进行少量开发，处理与互联网接入的内部应用接口。

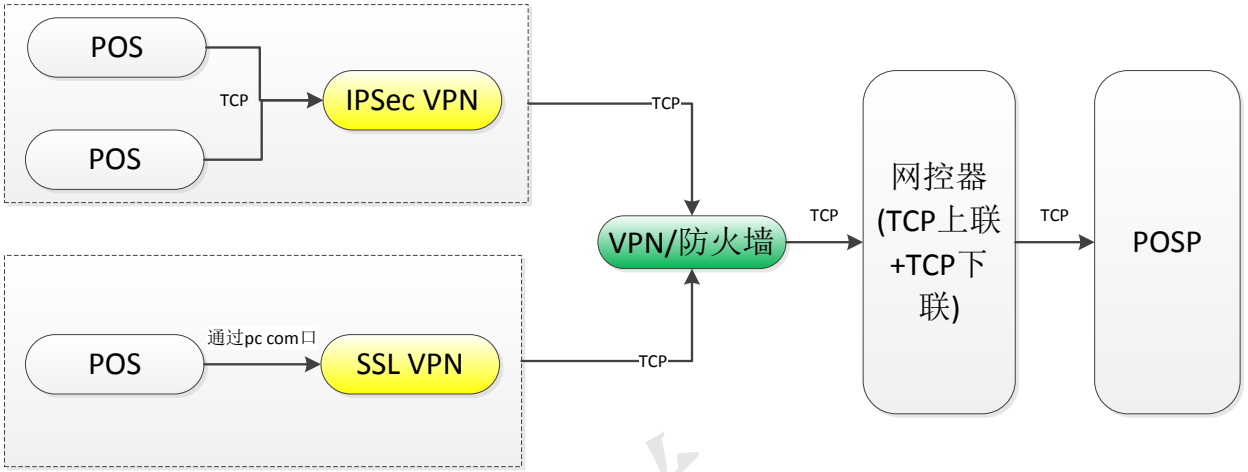
3.4.2 实施参考二



终端采用https单向认证接入互联网，系统平台开发httpserver及http与tcp协议转换器以满足POS终端支持互联网接入。具体实施要点如下：

1、 终端开发支持https单向认证，原8583报文或其它报文（例如脚本等）直接通过https进行交互；
2、 终端布放时安全下装平台CA根证书，https交互时通过CA根证书验证平台合法性；
3、 平台在F5上部署平台端证书，实现https单向认证接入以及报文转换；
4、 POSP平台前端增加http server及http与tcp协议转换器，协议转换后直接接入到POSP。

3.4.3 实施参考三

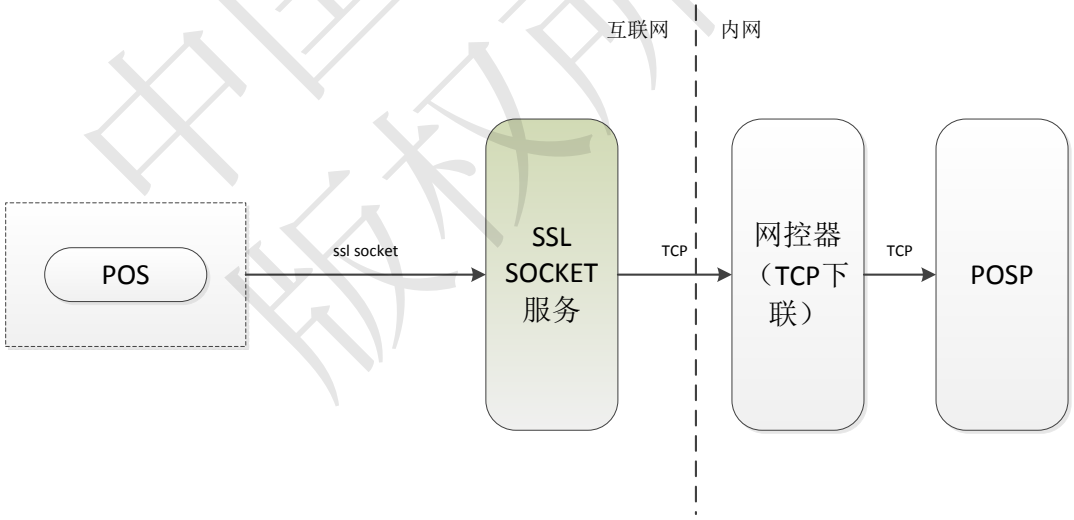


该方案主要针对大型连锁超市及家电零售企业等，终端和平台不需要软件改动，而是通过增加设备并将网络从专网DDN专线切换为互联网VPN专线，从而避免专线月租费开销。具体实施要点如下：

1、 商户网络新增VPN网络设备或串口转TCP/IP转换器、VPN客户端等，同时平台也相应增加相适应的VPN及防火墙；

2、 由商户网络的VPN相关软件及设备与服务端的VPN/防火墙建立安全隧道，以保障交互数据的安全性。

3.4.4 实施参考四



终端采用ssl socket接入互联网，系统平台增加ssl socket服务。具体实施要点如下：

1、 终端开发支持ssl socket,单向认证,原8583报文或其它报文(例如脚本等)直接通过ssl socket进行交互；

2、 终端布放时安全下装CA根证书，ssl socket交互时通过CA根证书验证平台合法性；

3、 平台在ssl socket服务上部署平台端证书，并需确保平台端证书安全性。

3.4.5 实施参考比较

实施参考三需要较大的硬件成本投入，主要针对具有内部局域网络的大型连锁超市，百货等；实施参考四采用ssl socket，但在互联网下搭建web服务进行http报文处理更具便捷性、更易部署；而实施参考一和实施参考二主要针对个体商户，实施成本较低。因此具体实施方案应以商户网络差异以及投入成本进行衡量，建议采用实施参考一和实施参考二。

4 接入方案二：SSL/TLS 双向认证方案

4.1 概述

本方案适用于终端直接采用SSL/TLS安全通讯协议接入互联网，且实施时选择的是双向认证。双向认证指的是在单向认证基础上增加系统对终端的合法性认证。

4.2 终端要求

终端除满足3.2相关要求外，还应满足以下要求：

——终端应对私钥进行安全管理，避免非法访问或修改；

——私钥由终端生成，其对应的公钥经过平台CA签名过后可用于校验终端合法性，同时私钥生成应不可预测，生成过程中应引入随机或伪随机值；

——当私钥的实例不再需要处于激活状态时，应将其清除；

——其它相关要求见《银联卡密码算法使用与密钥管理规范》（QCUP 058）。

4.3 平台要求

平台除满足3.3相关要求外，还应满足以下要求：

——平台应建立终端公钥证书的签发系统；

——平台应具备终端证书管理的功能，如导入、撤销等功能。

5 补充说明

交易报文层面，磁道信息、个人标识码（PIN）应被安全加密，应计算报文鉴别码（MAC），基于此可增加采用交易信息全报文加密等。应确保一机一密，各类信息的加解密密钥用途单一，且相互之间可严格区别，不复用。

6 用户体验设计建议

1、 终端宜方便操作者获取或查看MAC码；
2、 以太网通讯方式宜支持DHCP动态获取IP；
3、 终端宜灵活配置DNS，用于域名访问；
4、 终端支持SOCK5或HTTP代理协议，以便于需要设置代理服务器的局域网快速实现互联网接入；
5、 WLAN模块应提供WIFI连接功能，支持基础和点对点连接方式，支持开放连接、WPA-PSK加密连接。WLAN模块可以设置开机自动连接AP，终端显示WIFI连接状态。

7 总结

接入方案一单向认证未从传输层防范伪终端恶意攻击平台(交易安全通过叠加应用层密钥机制可保证），但对现有终端管理工作影响小，终端布放流程基本与现有保持一致；并且平台和终端仅需较少的改造工作量可达到POS终端支持互联网接入，安全上也满足规范要求。

接入方案二双向认证实现了平台对终端的认证，较好地解决伪终端问题并提高平台的健壮性，但需要建设配套的证书管理平台，证书管理复杂、实施周期较长。

具体方案选择上建议结合平台现状及技术基础架构，确定合适的方案进行实施，实现系统平台平稳过渡。另外，本《方案》提供的接入方案可有效地防止欺骗性攻击，对于穷举性、拒绝服务等暴力攻击手段和方法建议收单机构采取专业网络安全设备（例如防火墙等）进行防范。