Q/CUP

中 国 银 联 股 份 有 限 公 司 企 业 标 准

中国银联银行卡联网联合技术规范 V2.1
Token 支付方案

2015-XX-XX 发布　　2015-XX-XX 实施

中 国 银 联 股 份 有 限 公 司　发布

知识产权声明

中国银联股份有限公司（以下简称“中国银联”）对该规范文档保留全部知识产权权利，包括但不限于版权、专利、商标、商业秘密等。任何人对该规范文档的任何使用都要受限于在中国银联成员机构服务平台（http://member.unionpay.com/）与中国银联签署的协议之规定。中国银联不对该规范文档的错误或疏漏以及由此导致的任何损失负任何责任。中国银联针对该规范文档放弃所有明示或暗示的保证,包括但不限于不侵犯第三方知识产权。

未经中国银联书面同意，您不得将该规范文档用于与中国银联合作事项之外的用途和目的。未经中国银联书面同意，不得下载、转发、公开或以其它任何形式向第三方提供该规范文档。如果您通过非法渠道获得该规范文档，请立即删除，并通过合法渠道向中国银联申请。

中国银联对该规范文档或与其相关的文档是否涉及第三方的知识产权（如加密算法可能在某些国家受专利保护）不做任何声明和担保，中国银联对于该规范文档的使用是否侵犯第三方权利不承担任何责任，包括但不限于对该规范文档的部分或全部使用。

目　　次

前　　言

本标准由中国银联股份有限公司提出。
本标准由中国银联股份有限公司制定。

变更清单

序号	变更章节号	变更内容	变更原因	系统改造影响性分析（仅供机构参考）	变更人员	变更时间
1.	全文	全文	支持基于 token 支付创新产品	联机系统 清算系统	白玫	2015-5-22
2.						
3.						
4.						
5.						

中国银联银行卡联网联合技术规范 V2.1
Token 支付方案

1 范围

本方案适用于所有加入中国银联银行卡信息交换网络、使用支付标记化完成支付交易的境内入网机构。

本方案是对《中国银联银行卡联网联合技术规范V2.1》的补充修订方案，凡是本标准未提及内容，均按《中国银联银行卡联网联合技术规范V2.1》规定的内容执行。后续，待本方案试点运行稳定后，将合并入《中国银联银行卡联网联合技术规范V2.1》统一发布。

2 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。

Q/CUP 006 中国银联银行卡联网联合技术规范V2.1

Q/CUP XXX 中国银联支付标记化管理服务接口技术规范

3 术语和定义

3.1 支付标记 Payment Token

主账号（PAN） 的一个替代值，一般由 13 至 19 位的数字组成，该数值必须符合账号的基本验证规则，其中包括LUHN 算法校验。在银行卡支付交易中用支付标记替换卡号，用支付标记的有效期替换卡号有效期，不影响交易处理，增强了交易安全。

3.2 标记 BIN Token BIN

标记BIN 与卡BIN类似，主要用于在支付网络中路由，但不能和主账号PAN的BIN冲突。仅用于支付标记的发行，且属于特定的 BIN范围，并在BIN 表格中被相应标识。

3.3 标记服务提供方 Token Service Provider（TSP）

标记服务提供方是产生、维护标记的主体，它也负责标记请求方管理，并向其提供标记。负责支付标记化系统（TSP）的建设、维护以及运营，标记服务提供方作为支付标记的发行机构，有责任履行以下职责：

- 标记库的持续运行和维护
- 支付标记的生成与发布
- 安全应用和控制
- 支付标记数据准备
- 标记请求方的注册功能
- 建立及管理其自身的标记请求者API、标记库、标记提取平台及标记注册功能。
- 确保标记BIN 或标记BIN范围与传统卡号 BIN 不同，以防止 PAN 与标记的冲突。

3.4 标记请求方 Token Requestor（TR）

向标记服务提供方提交标记申请的机构。该机构可以是传统支付行业的参与者或者某类专业化服务提供方。在标记化系统中，标记服务提供方管理并唯一标识标记请求方。标记请求方的实体可以是以下参与方：

- 存留卡号信息的商户
- 收单机构、收单机构的外包服务方以及提供商户支付的网关服务方
- 移动设备或芯片制造商

— 数字钱包服务商
— 发卡机构

标记请求方需遵循标记服务提供方的管理标准、技术规范和入网申请流程。在成功注册后，标记请求方将被分配一个唯一的ID号码。结合不同的交易场景，一个标记请求方可以申请多个ID。

3.5 身份识别和验证 Identification and Verification （ID&V）

用于验证持卡人及其账户的有效性的方法，ID&V作为支付标记申请时一个重要环节，其结果直接决定了所申请的支付标记和原始主账号PAN之间的可信程度。

3.6 标记担保级别 Token Assurance Level

担保级别用于表示所申请的支付标记和其绑定的主账号PAN可信程度的值，该值受很多因素的影响，包括账户验证的结果、身份认证的结果、风险监控系统的评分等等，它也会受到标记存储位置等其它因素的影响。

担保级别在标记产生时由标记服务提供方根据一系列控制要素和验证结果综合判定；在标记产生之后，如果对该标记进行额外的 ID&V操作，标记的担保级别也可进行更新。

3.7 标记的域控

表示标记绑定的使用场景，比如特定的交易类型、支付渠道（例如仅 NFC）、商户名称、数字钱包服务提供方或者以上限定场景的任意组合。

3.8 标记的存储位置

支付标记位置的安全性将会影响该支付标记的担保级别。标记服务提供方需要定义标记的存储位置，并且负责对相关的标记请求方申请的存储位置执行检查。建议包括以下存储类型：

— 远程存储，例如大商户的服务器；
— SE存储，例如芯片，手机中的SE；
— 本地安全环境存储：例如TEE；
— 远程安全环境存储：如云SE；

3.9 去标记化

去标记化，是支付标记系统根据当前的交易场景在判断支付标记的有效性、域控以及交易金额限制等措施后，将其转换为原始主账号PAN的操作。

4 缩略语

ID&V	身份识别和验证（Identification and Verification）
PAN	主账号（Primary Account Number）
TR	标记请求方（Token Requestor）
TSP	标记服务提供方（Token Service Provider）

5 交易处理

5.1 交易说明

经CUPS转接的支付标记化交易是由终端向受理方发起，经CUPS转接，向发卡机构发送的金融支付类交易，包括消费类、预授权类、取现类、转账类、余额查询、账户验证。

5.2 交易处理流程

5.2.1 金融支付类交易

5.2.1.1 正常处理流程

受理方、发卡方与CUPS之间的交易正常处理流程，与基于PAN的交易正常处理保持一致。对于需CUPS向发卡方转发的请求类、通知类、手工类报文，CUPS将对报文进行去标记化处理。

5.2.1.2 异常处理流程

受理方、发卡方与CUPS之间的异常处理流程，与基于PAN的金融类交易异常处理保持一致。

当CUPS去标记化时，如发生系统、通讯等异常，CUPS将以应答码96向受理方返回拒绝应答，CUPS不再将交易报文转发至发卡方。

5.3 支持的交易类型

5.3.1 单信息交易

5.3.1.1 消费类

基于支付标记的消费类交易，包括各种应用场景的消费及其后续撤销、冲正、退货交易，其交易类型定义与基于PAN的消费类交易定义保持一致。

消费类交易关键域取值与基于PAN的消费类交易定义一致：

表1 消费类交易关键域取值

交易类型	消息类型（请求/应答）	第 3 域取值	第 25 域取值	其他域取值说明
消费（一次性付款）	0200/0210	00x000	00	
消费（一次性付款）冲正	0420/0430	00x000	00	
消费（一次性付款）撤销	0200/0210	20x000	00	
消费（一次性付款）撤销冲正	0420/0430	20x000	00	
MOTO 消费	0200/0210	00x000	08	
MOTO 消费冲正	0420/0430	00x000	08	
MOTO 消费撤销	0200/0210	20x000	08	
MOTO 消费撤销冲正	0420/0430	20x000	08	
消费（分期付款）	0200/0210	00x000	64	
消费（分期付款）冲正	0420/0430	00x000	64	
消费（分期付款）撤销	0200/0210	20x000	64	
消费（分期付款）撤销冲正	0420/0430	20x000	64	
消费（积分）	0200/0210	00x000	65	
消费（积分）冲正	0420/0430	00x000	65	
消费（积分）撤销	0200/0210	20x000	65	
消费（积分）撤销冲正	0420/0430	20x000	65	
消费（信用卡还款）	0200/0210	00x000	00	F18=9498
消费（信用卡还款）冲正	0420/0430	00x000	00	
退货（联机）	0220/0230	20x000	00	
MOTO 退货（联机）	0220/0230	20x000	08	
分期付款退货（联机）	0220/0230	20x000	64	
手工退货（包含查找到原始交易和无法查找到原始交易两种）	0220	20x000	00	F60.2.5=12
自助消费	0200/0210	00X000	00	F60.3.5=2
自助消费撤销	0200/0210	20x000	00	
自助消费撤销冲正	0420/0430	20x000	00	
自助消费冲正	0420/0430	00X000	00	

基于支付标记的消费类交易，清算方式与基于PAN的消费类交易清算方式保持一致。

5.3.1.2 预授权类

基于支付标记的预授权类交易，包括各种应用场景的预授权及其后续完成、撤销、冲正交易，其交易类型定义与基于PAN的预授权类交易定义保持一致。

预授权类交易关键域取值与基于PAN的预授权类交易定义一致：

表2　预授权类交易关键域取值

交易名称	消息类型（请求/应答）	第 3 域取值	第 25 域取值	其他域取值说明
预授权	0100/0110	03x000	06	
人工预授权	0100/0110	03x000	06	F60.2.5=14
MOTO 预授权	0100/0110	03x000	18	
预授权撤销	0100/0110	20x000	06	
手工预授权撤消	0100/0110	20x000	06	F60.2.5=12
MOTO 预授权撤销	0100/0110	20x000	18	
手工 MOTO 预授权撤销	0100/0110	20x000	18	F60.2.5=12
预授权冲正	0420/0430	03x000	06	
人工预授权冲正	0420/0430	03x000	06	F60.2.5=14
MOTO 预授权冲正	0420/0430	03x000	18	
预授权撤销冲正	0420/0430	20x000	06	
手工预授权撤消冲正	0420/0430	20x000	06	F60.2.5=12
MOTO 预授权撤销冲正	0420/0430	20x000	18	
手工 MOTO 预授权撤销冲正	0420/0430	20x000	18	F60.2.5=12
预授权完成（请求）	0200/0210	00x000	06	
预授权完成（通知）	0220/0230	00x000	06	
手工预授权完成	0220	00x000	06	F60.2.5=12
MOTO 预授权完成（请求）	0200/0210	00x000	18	
MOTO 预授权完成（通知）	0220/0230	00x000	18	
手工 MOTO 预授权完成	0220	00x000	18	F60.2.5=12
预授权完成撤销（请求）	0200/0210	20x000	06	
MOTO 预授权完成撤销（请求）	0200/0210	20x000	18	
预授权完成（请求）冲正	0420/0430	00x000	06	
MOTO 预授权完成（请求）冲正	0420/0430	00x000	18	
预授权完成（请求）撤销冲正	0420/0430	20x000	06	
MOTO 预授权完成（请求）撤销冲正	0420/0430	20x000	18	
结算通知	0220/0230	00x000	06	
MOTO 结算通知	0220/0230	00x000	18	
自助预授权	0100/0110	03X000	06	F60.3.5=2
自助预授权冲正	0420/0430	03X000	06	
自助预授权撤销	0100/0110	20X000	06	
自助预授权撤销冲正	0420/0430	20X000	06	
自助预授权完成（请求）	0200/0210	00X000	06	
自助预授权完成（请求）冲正	0420/0430	00X000	06	
自助预授权完成（通知）	0220/0230	00X000	06	
自助预授权完成撤销	0200/0210	20X000	06	
自助预授权完成撤销冲正	0420/0430	20X000	06	

基于支付标记的预授权类交易，清算方式与基于PAN的预授权类交易清算方式保持一致。

5.3.1.3 取现类

基于支付标记的取现类交易，包括各种应用场景的取现及其后续冲正交易，其交易类型定义与基于PAN的取现类交易定义保持一致。

取现类交易关键域取值与基于PAN的取现类交易定义一致：

表3 取现类交易关键域取值

交易类型	消息类型（请求/应答）	第 3 域取值	第 25 域取值	其他域取值说明
ATM 取现	0200/0210	01x000	02	F60.2.5=01
柜面取现	0200/0210	01x000	00	F60.2.5=06
POS 取现	0200/0210	01x000	00	
助农取现	0200/0210	01x000	00	F18=6051
ATM 取现冲正	0420/0430	01x000	02	F60.2.5=01
柜面取现冲正	0420/0430	01x000	00	F60.2.5=06
POS 取现冲正	0420/0430	01x000	00	
助农取现冲正	0420/0430	01x000	00	F18=6051

基于支付标记的取现类交易，清算方式与基于PAN的取现类交易清算方式保持一致。

5.3.1.4 转账类

基于支付标记的转账类交易，包括各种应用场景的转账、转出、转入、转入确认、转出冲正交易，其交易类型定义与基于PAN的转账类交易定义保持一致。

转账类交易关键域取值与基于PAN的转账类交易定义一致：

表4 转账类交易关键域取值

交易类型	消息类型（请求/应答）	第 3 域取值	第 25 域取值	其他域取值说明
转账受理（转出方付费）	0200/0210	40x000	00	
转账拆分的转出（转出方付费）	0200/0210	46x000	00	
转账拆分的转入（转出方付费）	0200/0210	47x000	00	
转入确认（转出方付费）	0220/0230	47x000	00	
转出冲正（转出方付费）	0420/0430	46x000	00	
助农转账受理（转出方付费）	0200/0210	40x000	00	F18=6051
助农转账拆分的转出（转出方付费）	0200/0210	46x000	00	
助农转账拆分的转入（转出方付费）	0200/0210	47x000	00	
助农转入确认（转出方付费）	0220/0230	47x000	00	
助农转出冲正（转出方付费）	0420/0430	46x000	00	

基于支付标记的转账类交易，清算方式与基于PAN的转账类交易清算方式保持一致。

5.3.1.5 余额查询

基于支付标记的余额查询交易，包括各种应用场景的余额查询交易，其交易类型定义与基于PAN的余额查询交易定义保持一致。

余额查询交易关键域取值与基于PAN的余额查询交易定义一致：

表5 余额查询交易关键域取值

交易类型	消息类型	第 3 域取	第 25	其他域取值说

	（请求/应答）	值	域取值	明
ATM 余额查询	0200/0210	30x000	02	F60.2.5=01
助农取款余额查询	0200/0210	30x000	00	F18=6051 F60.2.5=03 、11、17
其他余额查询	0200/0210	30x000	00	

基于支付标记的余额查询交易，清算方式与基于PAN的余额查询交易清算方式保持一致。

5.3.1.6 账户验证

基于支付标记的账户验证交易，包括各种应用场景的账户验证交易，其交易类型定义与基于PAN的账户验证交易定义保持一致。

账户验证交易关键域取值与基于PAN的账户验证交易定义一致：

表6 账户验证交易关键域取值

交易类型	消息类型（请求/应答）	第 3 域取值	第 25 域取值	其他域取值说明
账户验证	0100/0110	33x000	00	

基于支付标记的账户验证交易，清算方式与基于PAN的账户验证交易清算方式保持一致。

5.3.2 双信息交易

5.3.2.1 授权类

基于支付标记的授权类交易，包括各种应用场景的授权及其后续撤销、冲正交易，其交易类型定义与基于PAN的授权类交易定义保持一致。

授权类交易关键域取值与基于PAN的授权类交易定义一致：

表7 授权类交易关键域取值

交易名称	消息类型（请求/应答）	第 3 域取值	第 25 域取值	其他域取值说明
消费授权（一次性付款）	0100/0110	00x000	00	
MOTO授权	0100/0110	00x000	08	
消费授权（一次性付款）撤销	0100/0110	20x000	00	
MOTO授权撤销	0100/0110	20x000	08	
消费授权（一次性付款）冲正	0420/0430	00x000	00	
MOTO授权冲正	0420/0430	00x000	08	
消费授权（一次性付款）撤销冲正	0420/0430	20x000	00	
MOTO授权撤销冲正	0420/0430	20x000	08	
自助授权	0100/0110	00X000	00	F60.3.5=2
自助授权冲正	0420/0430	00X000	00	
自助授权撤销	0100/0110	20X000	00	
自助授权撤销冲正	0420/0430	20X000	00	

5.3.2.2 余额查询

基于支付标记的余额查询交易，包括各种应用场景的余额查询交易，其交易类型定义与基于PAN的余额查询交易定义保持一致。

余额查询交易关键域取值与基于PAN的余额查询交易定义一致：

表8 余额查询交易关键域取值

交易类型	消息类型（请求/应答）	第 3 域取值	第 25 域取值	其他域取值说明
余额查询	0100/0110	30x000	00	

基于支付标记的余额查询交易，清算方式与基于PAN的余额查询交易清算方式保持一致。

6 报文接口

6.1 报文域

6.1.1 60.2.7 域

在60.2.7域（芯片卡授权可靠性指示）新增取值，用于标识该交易使用银联提供的token服务。

域	属性	取值	取值说明
60.2.7	n1	4	用于为发卡方指示该交易使用银联提供的token服务。

6.1.2 63 域

6.1.2.1 变量属性

ansb...512（LLLVAR），即3字节长度值＋最大512个字节(字母、数字和特殊字符)的数据。

6.1.2.2 域描述

本域为多用法域，用于传递交易中的安全、风险控制相关信息。当前使用的用法包括：

用法SM：用作传递国密算法相关数据（具体参见国密算法配套标准）。

用法TK：用作传递Token相关数据（本规范中定义）。

整个域的总体格式为：

<域总长度><用法ID1><用法ID1长度><用法ID1取值>.....<用法IDn><用法IDn长度><用法IDn取值>

根据交易场景不同，本域中的用法可单独使用，也可组合使用。

表9 63 域属性定义

域总长度	用法ID	用法长度	用法取值
n3	an2	n3	ansb变长，最大507字节

表10 63 域用法定义

用法 ID	用法 ID 中文名称	用法取值格式	说明
TK	**标记支付信息**	**TLV1+TLV2+.....+TLVn** 根据不同的应用产品包含不同的子域，每个子域由tag标签(T)，子域取值的长度(L)和子域取值(V)构成，子域传递无排序要求。 **TLV 格式定义与报文 55 域中的 TLV 格式定义保持一致，具体参见《中国银联银行卡联网联合技术规范 V2.1 第 2 部分报文接口规范》中 55 域的 TLV 格式定义。**	**用于在金融支付类交易中传递 Token 相关数据**
注：对于规范中定义的每个用法及其所有子域 tag，发卡方和受理方必须能够支持接收，包括不能识别或不期望收到的用法及其子域 tag，对于不能识别或不期望收到的用法及其子域 tag，发卡方和受理方可忽略并继续处理本域中的其他用法或本用法中的其他子域 tag。			

6.1.2.3 用法 TK

6.1.2.3.1 用法 TK 子域定义

表11 用法 TK 子域列表

<table>
<tr><th>子域名称</th><th>子域 tag
标签值</th><th>子域属性</th><th>子域说明</th></tr>
<tr><td>是否验证过
token 相关信息</td><td>01</td><td>an1</td><td>根据是否验证基于 token 的磁道或芯片信息（即验证报文域 F23、F35、F36、F45、F55）填写本域。取值如下：
0-未验证（表示基于 token 的磁道、芯片信息由发卡方产生）
1-验证通过</td></tr>
<tr><td>Token</td><td>02</td><td>an..19(LLVAR)</td><td>由 TSP 生成的 token</td></tr>
<tr><td>Token 有效期</td><td>03</td><td>an4(YYMM)</td><td>由 TSP 设定的 token 有效期</td></tr>
<tr><td>Token 担保级别</td><td>04</td><td>an..2(LLVAR)</td><td>由 TSP 根据风险评估，分配的 token 担保级别，取值范围：0~99</td></tr>
<tr><td>token 应用场景标识</td><td>05</td><td>n2</td><td>由 TR 提供的 token 应用场景标示，取值如下：
01- SE
02- HCE
03- 二维码
04- 大商户（COF）
05- 数字钱包</td></tr>
<tr><td>TRID</td><td>06</td><td>an8..11(LLVAR)</td><td>在 TR 注册时，由 TSP 分配，是 TR 的唯一编号。</td></tr>
<tr><td>QRC_DATA</td><td>07</td><td>ans..32(LLVAR)</td><td>二维码支付时，基于 token 生成的二维码验证信息。</td></tr>
<tr><td>产品标识</td><td>08</td><td>ansb4</td><td>token 申请时，由 TR 填写的产品标识，在支付交易中，CUPS 在去标记化时获取相应取值发往发卡方。如 TR 申请 token 时，未提交产品标识，则在支付交易中，该子域不出现。
该字段取值分为两段：
前 1 个字节，表示产品大类；后 3 个字节，表示产品细类，取值如下表定义：
<table>
<tr><th>序号</th><th>前 1 个字节属性及取值</th><th>后 3 个字节属性及取值</th></tr>
<tr><td>1</td><td>属性：ans
取值：
1-移动支付产品</td><td>属性：b
取值：参见《中国银联移动支付技术规范 应用卷 第 2 部分 用于可信服务管理平台的 PBOC 应用个人化规范》中对 9F63 第 10~12 字节的定义</td></tr>
</table>
</td></tr>
</table>

6.1.2.3.2 金融支付类交易中用法 TK 子域的传递要求

表12 金融支付类交易报文中用法 TK 子域的传递要求

子域名	子域	子域属性	各子域的传递要求	说明

称	tag 标签值		AC	SW	IS	SW	
银联是否验证过 token 相关信息	**01**	an1		M+			
Token	**02**	an..19(LLVAR)		M+			当受理方上送基于 token 的交易时，本域出现。
Token 有效期	**03**	an4(YYMM)		M+			当受理方上送基于 token 的交易时，本域出现。
Token 担保级别	**04**	an..2(LLVAR)		M+			当受理方上送基于 token 的交易时，本域出现。
token 应用场景标识	**05**	**n2**		M+			当受理方上送基于 token 的交易时，本域出现。
TRID	**06**	an8..11(LLVAR)		M+			当受理方上送基于 token 的交易时，本域出现。
QRC_DATA	**07**	ans..32(LLVAR)	C6	C6			二维码支付交易中，本域出现。 当 QRC_DATA 由银联系统产生时，本域不传递给发卡方。 当 QRC_DATA 由发卡方产生时，本域透传给发卡方。
产品标识	**08**	ansb4		C6+			当 TR 申请 token 时提交了产品标识，则本域出现。

6.2 报文格式

基于token的交易报文格式同基于PAN的交易。

以下仅列出基于Token支付交易的部分域传递和域取值的情况，其他未说明的域请参照原基于PAN的交易报文格式。

表13 金融支付类交易 token 相关报文域传递要求

报文域	域名称	格式	AC	SW	IS	SW	说明
2	主账号	n..19(LLVAR)	M	C16	M	C16	基于 token 的支付交易，银联系统将对本域进行相应的转换： 1、对于受理方发送的请求报文，本域存放 token 号，银联系统将 token 号转换为真实 PAN 号发送给发卡方。 2、对于发卡方返回的应答报文，本域存放真实 PAN 号，银联系统会将 PAN 号转换为 token 号返回给受理方。
14	卡有效期	n4(YYMM)	O	C6	M	C6	基于 token 的支付交易，银联系统将对本域进行相应的转换： 1、对于受理方发送的请求报文，本域存放 token 有效期。如果 token 申请时已提交真实 PAN 有效期，则银联系统将 token 有效期转换为真实 PAN

							有效期发送给发卡方。如果 token 申请时未提交真实 PAN 有效期，则银联系统将删除 14 域，不再发送给发卡方。 2、对于发卡方返回的应答报文，本域存放 PAN 有效期，银联系统将有 PAN 效期转换为 token 有效期返回给受理方。
22	服务点输入方式码	n3	M	→			本域由受理方填写 token 真实的输入方式，银联系统将原样转发本域取值至发卡方。 22 域前两位取值说明如下： 磁条输入：02、90 芯片输入：05、07、95、98 二维码输入：04（对应的 60.3.6 域交易介质取值为 7）
23	卡序列号	n3	C51	C6	C0	C6	基于 token 的支付交易，本域将存放 token 对应的序列号。 当 22 域前两位取值为 05、07、95、98 时，本域出现。 银联系统将对本域进行相应的转换： 1、对于受理方发送的请求报文，如基于 token 的芯片信息由发卡方产生，则银联系统将该域转发至发卡方；如基于 token 的芯片信息非发卡方产生，银联系统不将该域转发至发卡方。 2、对于发卡方返回的应答报文，如发卡方收到的请求报文中本域存在，则在应答报文中原样返回本域，银联系统透传本域至受理方；如发卡方收到的请求报文中本域不存在，则在应答报文本域也无需返回，如银联系统收到的请求报文中本域存在，则将请求报文中该域取值放入应答报文转发至受理方。
35	第二磁道数据	z..37(LLVAR)	C1	C6			在受理请求报文中，当 22 域前两位取值为 02、05、07、90、95、98 时，本域出现。基于 token 的支付交易，本域将存放 token 对应的磁道信息。 如基于 token 的磁道信息由发卡方产生，则银联系统将该域转发至发卡方；如基于 token 的磁道信息非发卡方产生，且发卡方需要该信息，则银联系统将该域转发至发卡方，并根据与发卡方约定的规则（基于 PAN 或 token，CVN 的产生规则等）填写磁道信息；如基于 token 的磁道信息非发卡方产生，且发卡方不需要该信息，银联系统不将该域转发至发卡方。
36	第三磁道数据	z...104(LLLVAR)	C2	C6			当 22 域前两位取值为 02、05、07、90、95、98，且三磁信息存在时，本域出现。 其他定义同上。

45	第一磁道数据	z..76(LLVAR)		C6			在跨境交易中，境外受理方可能会上送该域。 其他定义同上。
55	基于UICS 借贷记标准的 IC 卡数据域	ansb...255(LLLVAR)	各子域的传递要求参见相应的IC卡交易报文格式	C6			基于 token 的支付交易，本域将存放 token 对应的芯片信息。 当 22 域前两位取值为 05、07、95、98 时，本域出现。 本域由受理方填写。如基于 token 的芯片信息由发卡方产生，则银联系统将该域转发至发卡方；如基于 token 的芯片信息非发卡方产生，银联系统不将该域转发至发卡方。 应答报文中本域将不出现，即基于 token 的芯片交易，应答报文中将不包含 ARPC 和脚本，受理侧也无需校验 ARPC 和处理脚本。
60.2.7	IC 卡验证可靠性标志	n1	M	C6	M	C16	受理请求报文按原有处理逻辑填写本域。 银联系统如对该交易提供了 token 服务，则将该域填写新定义取值转发给发卡方。 发卡应答报文原样返回该域取值。 银联系统在给受理方应答时，需将受理请求上送的该域取值原样返回给受理方。
63	安全风险信息	ansb…512（LLLVAR）	各子域传递要求参见本规范 6.1.2.3.2				若银联系统作为 token 的服务提供方（即 TSP），且机构支持接收 token 相关信息时，则该 TK 用法出现。对于转出转账报文，如果转出卡为银联提供的 token，则本域在转出转账报文中出现。对于转入转账报文，如果转入卡为银联提供的 token，则本域在转入转账报文中出现。 若为二维码交易，当发卡行作为 TSP，且机构支持接收 token 相关信息时，则 TK 用法出现（仅包含 QRC_DATA 数据）。

基于token的转账交易，F102、F103域的传递要求同基于PAN的转账交易，取值说明如下：

对于转账报文，请求中如果转出卡或转入卡均使用token，或仅有一方使用token，则对应的F102、F103填写对应的token或PAN，应答报文原样返回；

对于转出转账报文、转入转账报文、转出冲正、转入确认报文，请求和应答中的F102、F103均填写PAN。

7 清算处理

7.1 清算文件概述

基于Token支付交易与基于PAN的交易在清算方式和计费规则上无变化，仅在清算文件中增加传递Token相关信息。

7.2 受理侧涉及的文件列表

表14 跨行交易清算文件

文件中文含义	文件名称	文件发送方	文件接收方	记录格式代码
收付费文件	INDYYMMDD??FCP	CUPS	入网机构	FCP
一般交易受理方流水文件（新）	INDYYMMDD??ACOMN	CUPS	入网机构	COMN
转账交易受理方流水文件	INDYYMMDD??ATFL	CUPS	入网机构	TFL
差错交易受理方流水文件（新）	INDYYMMDD??AERRN	CUPS	入网机构	ERRN
收单机构联机/电子现金脱机交易周期计费流水文件（包含跨行清算和代理清算）	INDYYMMDD??APEDA	CUPS	入网机构	COMA
收单机构差错交易周期计费流水文件(包含跨行清算和代理清算）	INDYYMMDD??AERRPEDA	CUPS	入网机构	ERRA
品牌服务费受理方流水文件	INDYYMMDD??ALFEE	CUPS	入网机构	LFE
追偿清算受理方流水文件	INDYYMMDD??AFMCZ	CUPS	入网机构	FMC

表15 代理清算文件

文件中文含义	文件名称	文件发送方	文件接收方	记录格式代码
银联代理清算收单机构一般交易流水文件	INDYYMMDD??ACOMA	CUPS	入网机构	COMA
银联代理清算收单机构差错交易流水文件	INDYYMMDD??AERRA	CUPS	入网机构	ERRA
收单机构联机/电子现金脱机交易周期计费流水文件（包含跨行清算和代理清算）	INDYYMMDD??APEDA	CUPS	入网机构	COMA
银联代理清算收单机构差错交易周期计费流水文件	INDYYMMDD??AERRPEDA	CUPS	入网机构	ERRA
银联代理清算收单机构商户挂账交易明细文件	INDYYMMDD??ZHAC	CUPS	入网机构	ZM
银联代理清算商户交易流水文件（日间\日终）	AINSYYMMDD??MDALL+商户代码	CUPS	银联代理清算商户	ZM
银联代理清算商户交易周期计费流水文件	AINSYYMMDD??MDALLPED+商户代码	CUPS	银联代理清算商户	ZM
银联代理清算受理方服务机构交易流水文件	AINSYYMMDD??ASDALL	CUPS	服务机构	ZS
银联代理清算受理方服务机构交易周期计费流水文件	AINSYYMMDD??ASDALLPED	CUPS	服务机构	ZS

7.3 发卡侧涉及的文件列表

表16 跨行交易清算文件

文件中文含义	文件名称	文件发送方	文件接收方	记录格式代码
一般交易发卡方流水文件（新）	INDYYMMDD??ICOMN	CUPS	入网机构	COMN
转账交易转出方流水文件	INDYYMMDD??OTFL	CUPS	入网机构	TFL
转账交易转入方流水文件	INDYYMMDD??ITFL	CUPS	入网机构	

7.4 文件格式

7.4.1 文件格式概述

对于受理侧清算文件，文件格式均无变化，仅在清算文件中原主账号字段填写token号。

对于发卡侧清算文件，文件格式将在保留字段中新增Token相关信息，用以告知发卡机构Token与主账号的对应关系。**如果发卡机构不能识别新增的Token字段，可忽略该新增字段，不能因为新增字段而影响原清算文件的处理。**

7.4.2 流水文件记录格式

7.4.2.1 (COMN)一般交易流水文件记录格式（新）

COMN格式新增以下字段：

受理方交易流水格式				发卡方交易流水格式			
序号	描述	域号	类型长度	序号	描述	域号	类型长度
7	保留使用		n19	7	Token	63（TK）	n19
8	保留使用		ans106	8	保留使用		ans106

7.4.2.2 (TFL)转账交易流水文件记录格式（新）

TFL格式新增以下字段：

受理方交易流水格式				发卡方交易流水格式			
序号	描述	域号	类型长度	序号	描述	域号	类型长度
34	保留使用		n19	34	Token	63（TK）	n19
35	保留使用		ans276	35	保留使用		ans276

8 安全传输

8.1 安全概述

基于Token支付交易的加解密算法保持不变，具体参考《中国银联银行卡联网联合规范V2.1 第4部分数据安全传输控制规范》。

8.2 PIN BLOCK

对于带主账号异或的PIN BLOCK计算，增加如下说明：

基于token的支付交易，对于受理机构，使用Token号参与PIN BlOCK计算；对于发卡机构，使用真实卡号参与PIN BlOCK计算。

8.3 MAC 计算

对于参与MAC计算的数据元集，增加说明：

基于token的支付交易，对于受理机构，使用Token号参与MAC计算；对于发卡机构，使用真实卡号参与MAC计算。

9 通讯接口

基于Token的支付交易，CUPS通讯接口无变化，具体参考《中国银联银行卡联网联合规范V2.1 第5部分 通讯接口规范》。

10 机构影响性分析

10.1 受理侧改造

可选改造。

受理机构如选择支持token业务用于二维码支付，必选改造。

序号	改造点	改造影响分析
1.	联机交易	当为二维码支付场景时，受理侧需在请求报文中发送QRC_DATA信息。
2.	清算文件	无影响

10.2 发卡侧改造

可选改造。

发卡机构如选择支持Token业务，必选改造。

序号	改造点	改造影响分析
1.	联机交易	1、 联机交易中，当基于token的磁道、芯片信息非发卡机构生成，且发卡方不需要磁道信息时，Token相关信息（F23、F35、F36、F45、F55）将不再发送给发卡方，而此时报文22域仍填写原支付输入方式，发卡机构不能根据22域取值校验卡片信息（F23、F35、F36、F45、F55）。 2、 联机交易中，当基于token的磁道、芯片信息非发卡机构生成，且发卡方需要磁道信息时，Token相关信息（F35、F36、F45）将根据与发卡方约定的规则填写，并发送给发卡方，而此时报文22域取值不变。 3、 联机交易中，必选支持F63域。发卡机构可不解析F63域中的具体子域，但不能因F63域的存在或F63域新增子域而引起系统宕机或拒绝交易。 4、 联机交易中，必选支持F60.2.7域取值4。发卡机构可不解析F60.2.7域中的具体取值，但不能因F60.2.7域取新值而引起系统宕机或拒绝交易。
2.	清算文件	清算文件中，必选支持新增token号字段。发卡机构可不识别新增的token号，但不能因清算文件新增字段而导致系统宕机或无法清算。

参考文献

[1] EMVCo Payment Tokenisation Specification Technical Framework 1.0