ICS 35.240.40
A 11

JR

中华人民共和国金融行业标准

JR/T 0149—2016

中国金融移动支付 支付标记化技术规范

China financial mobile payment—Payment tokenization specification

2016-11-09 发布　　2016-11-09 实施

中国人民银行　发布

目　次

前　言

本标准按照GB/T 1.1—2009给出的规则起草。

本标准由中国人民银行提出。

本标准由全国金融标准化技术委员会（SAC/TC 180）归口。

本标准负责起草单位：中国人民银行科技司、中国金融电子化公司。

本标准参加起草单位：中国工商银行、中国农业银行、中国银行、中国建设银行、招商银行、中信银行、中国银联股份有限公司、蚂蚁金融服务集团、财付通支付科技有限公司、京东金融、中移电子商务有限公司、北京中金国盛认证有限公司、中金金融认证中心有限公司、银行卡检测中心、工业和信息化部计算机与微电子发展研究中心（中国软件评测中心）、信息产业信息安全测评中心。

本标准主要起草人：李伟、王永红、陆书春、李兴锋、曲维民、邬向阳、杨倩、王禄禄、周皓、蒋慧科、吴永强、黄本涛、王欢、赵哲、汤沁莹、贾铮、刘运、王兆国、罗鹏飞、卢婷、连宾雄、杨明、范俐捷、盛莹、同勇、王晓月、陈泽智、李明婕、戚小朝、李斌、刘栋、落红卫、方海峰、张谦、周缅、李茂材、付博、孙霄、丁晓强、阮森灵、罗乐、姜名峰、刘婧雯、黄江、许自强、叶强林、高志民、高强裔、白阳、郑晓娟、孙茂增、魏博锴、宋铮、黄晓培、王冠华。

引　言

近年来，国内商业银行、非银行支付机构等为保护支付敏感信息、提升支付安全，防范信息泄露和欺诈交易，在移动支付业务中逐步引入了支付标记化（Payment Tokenization）技术，通过支付标记（Token）代替银行卡卡号、非银行支付机构支付账户等支付要素进行交易，并对标记的应用范围加以限定，从源头遏制信息泄露，最大程度上保障用户交易安全。为落实《中国人民银行关于进一步加强银行卡风险管理的通知》（银发〔2016〕170号）要求，引导和规范各机构应用支付标记化技术，特制定本标准。

中国金融移动支付 支付标记化技术规范

1 范围

本标准提出了支付标记化技术的基本架构，规定了应用支付标记化技术的系统接口、安全、风险控制等要求。

本标准适用于从事支付标记化系统建设或服务运营的商业银行、非银行支付机构、支付转接清算机构、商户等机构。

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。

JR/T 0071—2012 金融行业信息系统信息安全等级保护实施指引

《中国人民银行关于进一步加强银行卡风险管理的通知》（银发〔2016〕170号，2016年6月15日）

3 术语和定义

下列术语和定义适用于本文件。

3.1

支付账号 payment account

具有金融交易功能的银行账户、非银行支付机构支付账户的编码，及银行卡卡号。

3.2

支付标记 payment token（Token）

作为支付账号等原始交易要素的替代值，用于完成特定场景支付交易。

3.3

支付标记化 payment tokenization

用支付标记替换支付账号等原始交易要素的过程。

3.4

去标记化 de-tokenization

标记服务提供方根据当前交易场景验证支付标记有效性后，将其还原为支付账号等原始交易要素的过程。

3.5

标记服务提供方 token service provider

支付标记的发行机构，负责支付标记生命周期管理，提供支付标记化、去标记化等服务。

3.6

标记有效期 token expiry date

支付标记使用的有效时间，应小于或等于支付账号等原始交易要素有效期。

3.7

支付标记发行机构识别码 token issuer identification number

唯一标识支付标记发行机构的编码。

3.8

标记请求方 token requestor

向标记服务提供方提交标记申请的机构。

3.9

域控 token domain restriction controls

标记服务提供方在生成标记时预设的一组参数，用于确定标记的使用范围，如交易类型、交易金额、使用次数、支付渠道等。

4 符号和缩略语

下列符号和缩略语适用于本文件。

C 有条件的选择项
M 必选项
O 可选项
R 应答中应返回
VAR 可变长度域
a 字母a～z
n 数字0～9
s 特殊字符
an 字母和数字字符
ans 字母、数字和特殊字符
as 字母和特殊字符
ns 数字和特殊字符
ARQC 授权请求密文（Authorization Request Cryptogram）
ID&V 身份识别和验证（Identification and Verification）
PA 支付账号（Payment Account）
TIN 支付标记发行机构识别码（Token Issuer Identification Number ）
TR 标记请求方（Token Requestor）
TSP 标记服务提供方（Token Service Provider）

5 系统实现

5.1 体系架构

支付标记化体系架构描述了支付标记化的主要角色，规定了标记请求方(TR)、标记服务提供方(TSP)与传统支付流程的关系和数据交互接口，明确了各角色如何共同为用户提供标记服务。图1描述了支付标记化体系架构。

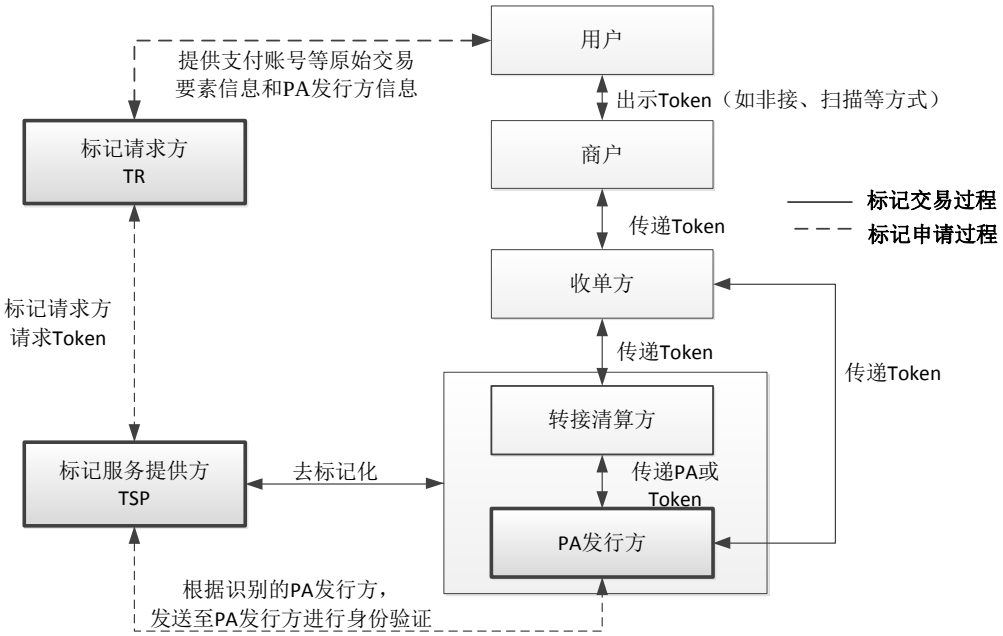

图1 支付标记化体系架构

其中，TSP是该标记化框架的核心角色，提供Token的生成、管理、去标记化等功能，负责TR的注册和管理。TSP对PA发行方信息进行维护，确保PA发行方信息的真实性和有效性，并向标记请求方、业务需求方提供数据接口。

TSP角色的实体可由商业银行、非银行支付机构、支付转接清算机构等承担。

TR向TSP申请Token，并提供支付账号等原始交易要素和PA发行方信息。

同一主体可承担TSP、TR、PA发行方、收单方等多个角色。

5.2 TSP 系统功能

TSP系统应具备以下功能：

——标记库的持续运行和维护；

——Token 的生成与发布；

——Token 生命周期管理，包括属性更新和状态管理等；

——去标记化处理；

——判断 Token 状态是否正常，正确应答关联方请求；

——安全应用和控制，保证信息存储、传输和处理的安全性；

——域控处理，包括交易金额、交易渠道、商户范围等，具体域控要素可参考附录 A 表 A.1、A.2、A.3 中“是否为域控要素”中的说明；

——TR 的管理，包括 TR 合法性验证、注册、注销、业务风险通知等；

——建立及管理与 TR、业务需求方的数据接口；

——欺诈信息共享，TSP 与 PA 发行方、TSP 间共享欺诈信息。

5.3 TR 管理

5.3.1 TR 注册

TSP应根据业务需要制定TR的申请和注册流程，图2描述了TR注册流程。

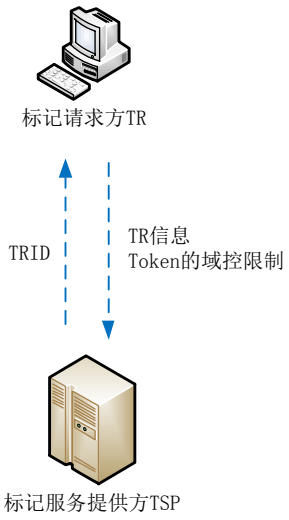

图2 TR 注册流程

TR向TSP提交注册信息，由TSP进行审核。审核通过后，TSP为TR分配唯一的ID（TRID），并记录该TRID对应的标记域控参数，用于后续的交易验证。

TR注册信息包括TR身份信息、标记域控信息，具体内容可参照附录A。

5.3.2 TR 注销

TR可主动向TSP提出注销申请。如TR存在违反TSP管理要求的情况，TSP有权对TR予以强制注销。

TR注销后，TSP回收TRID，将该TR及其申请的Token做失效处理，TR应及时告知业务相关方，并对系统中存储的所有相关信息应进行脱密、销毁处理。

6 支付标记申请

6.1 申请流程

图3描述了支付标记的申请流程。

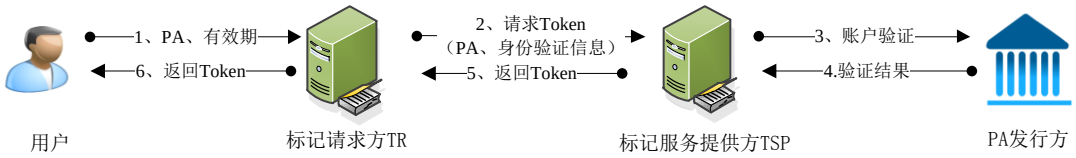

图3 支付标记申请流程

具体申请流程步骤说明如下：

步骤1：用户向TR提交支付账号等原始交易要素信息；

步骤2：TR向TSP申请Token；
步骤3：TSP向PA发行方验证账户信息及用户身份信息；
步骤4：PA发行方将验证结果返回至TSP；
步骤5：TSP生成Token，并返回给TR；
步骤6：TR向用户返回Token。

6.2 申请要素

TR提交的信息至少应包括：标记请求方标识码（即TRID），支付账号等原始交易要素（包括账号、有效期等），标记属性（域控属性、存储位置等）。相关申请要素参见附录A。

6.3 标记格式

6.3.1 Token 编码规则

Token长度范围为13至34位。Token由三部分组成：TIN、TSP自定义位、校验码。
不同的TSP应使用不同的TIN。TIN长度为6至12位。
应确保TIN在支付网络内的唯一性。
Token的最后n位是校验码（n由TSP自定义）。
TIN与校验码之间为TSP自定义位，由TSP自行赋值。

6.3.2 唯一性要求

TSP应确保Token的唯一性。TSP应确保Token在失效或注销之日起，在有可能影响后续关联交易的时间周期内不得重复被分配给其他用户。

6.4 标记属性

6.4.1 有效期

在Token生成过程中，由TSP根据TR申请的有效期、TR域控属性中允许的有效期、PA有效期等因素综合确定Token有效期，Token有效期应为以上三者中的最小值。

6.4.2 存储位置

TSP需要定义Token的存储位置，并且负责对相关TR申请Token的存储位置执行检查。存储类型包括但不限于：
——远程服务器存储，如商户的服务器；
——本地安全芯片存储，例如移动设备中的 SE；
——本地安全环境存储，例如 TEE；
——远程安全环境存储，例如云 SE（HCE 模式）；
——本地软件环境存储，例如移动设备中的客户端软件。
TSP应根据Token在用户端本地存储位置的差异为Token确定不同的有效期和使用次数。

6.5 身份验证

用户向TR申请Token后，TR将必要的用户身份验证信息上送TSP，TSP向PA发行方发起身份验证请求，验证用户身份。

应按照《中国人民银行关于进一步加强银行卡风险管理的通知》关于业务开通、交易安全等方面要求，采取必要的安全验证方式。

6.6 域控设置

Token申请时TSP应根据交易渠道、商户范围、身份验证强度等进行风险评估及交易权限控制，根据风险评估结果对Token的有效期、交易次数和交易金额等信息进行限制。

TR应综合设备标识、软件环境、设备保护能力等判断当前Token申请的风险程度，并根据风险程度级别为Token定义不同的申请授权时长和授权金额。

TR向TSP提出Token申请时，申请的Token域控属性应在TR域控属性范围内，且Token有效期应小于或等于PA有效期。TR可在Token失效前，根据具体应用场景，主动发起Token的延期或更新操作。

7 支付标记使用

7.1 标记交易

图4描述了收单方直联PA发行方的支付标记交易流程。

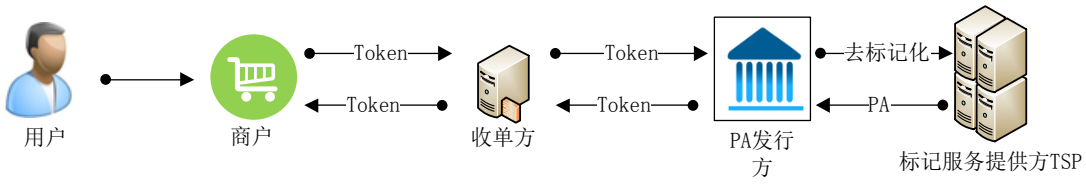

图4 支付标记的交易流程（收单方直连 PA 发行方）

图5描述了经转接清算方转接的支付标记交易流程。

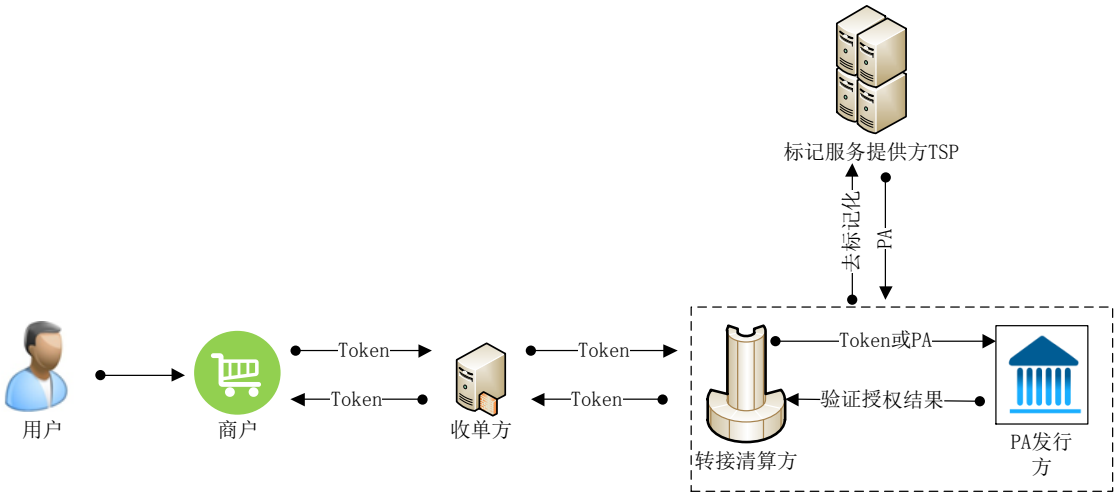

图5 支付标记的交易流程（经过转接清算方转接）

支付标记交易的处理流程与现有基于PA的交易处理流程一致，仅在去标记化操作时需要TSP完成标记的验证和还原。用户发起交易，商户将交易信息(包含用于识别交易的电子凭证信息，该凭证信息应与本次交易使用的Token一一对应)发送给收单方，收单方将交易信息发送至转接清算方（或直接发送到PA发行方），最后由PA发行方完成交易。在交易过程中可由PA发行方或转接清算方向TSP发起去标记化过程。而Token交易路由与PA的交易路由一致。TSP作为标记服务处理系统，完成Token与原PA的转换操作。

去标记化交易处理具体如下：

——去标记化过程中，需要对 Token 的有效性（有效期、标记状态等）进行验证，如果 Token 无效，应拒绝交易；

——TRID（标记请求方 ID）是一个控制数据元，应在交易中进行校验。如果交易报文中的 TRID 与 TSP 标记库中存储的该支付标记对应的 TRID 不匹配时，应拒绝交易；

——从交易报文中提取域控相关的数据元，并与 TSP 标记库中定义的交易域控元素比对，若不匹配，应拒绝交易；

——TSP 应根据交易类型进行交易数据验证（验磁、验 ARQC 授权请求密文等），确保交易信息安全可信。

退款处理具体如下：

——对于用户可以提供支付所用 Token 信息且该 Token 未失效的情况，商户直接使用 Token 发起退款交易。该退款交易传递到 TSP 进行去标记化处理，将该 Token 退款还原为 PA 的退款交易，并到 PA 发行方完成入账；

——对于用户无法提供 Token 信息或 Token 已失效的情况，用户提交支付过程中得到的交易电子凭证信息，由商户或收单方根据该电子凭证查询获取用于本次支付的 Token，并以该 Token 发起退款交易。TSP 通过去标记化处理转换为 PA 的退款交易，由 PA 发行方完成入账；

——对于用户否认标记支付行为的情况，由 TSP 和 PA 发行方协商处理。

7.2 交易要素

去标记化过程中，申请方向TSP提交的信息至少应包括标记属性（Token号、Token长度、有效期、TRID）、交易数据（交易时间、交易金额）等。TSP向申请方返回交易结果、Token关联的PA。相关交易要素参见附录A。

8 支付标记生命周期管理

8.1 状态管理

TR、PA发行方可作为直接发起方，向TSP发起Token状态管理类请求。Token状态管理包括：

——激活，将未激活状态的 Token 变更为已激活状态。

——锁定，由于设备遗失或被盗等原因，将 Token 与 PA 的映射关系临时失效。

——解锁，将锁定的 Token 的状态恢复正常，该 Token 与 PA 的映射关系被重新激活。

——注销，将 Token 与 PA 的映射关系解除，对应关系废止。具体场景包括但不限于设备遗失或被盗、PA 遗失或被盗、PA 欺诈警告、Token 欺诈警告。

8.2 属性管理

由于PA发行方更新PA及PA的属性信息，TSP应同步更新PA及标记相关属性信息，以及Token与该PA的映射关系。

9 风险控制要求

9.1 TSP 风险控制要求

TSP风险控制要求如下：

——应建立相关的风险管理制度，包括风险识别与分析、风控规则管理、风险事件处置等；

——应提供一段时间内的风险事件报表，或提供查询一段时间内的风险事件报表功能；
——应结合域控策略实现风险识别与防范；
——应对支付标记请求、去标记化等标记活动进行记录，用于审计；
——应对服务对象进行风险管理，服务对象包括商业银行、非银行支付机构、支付转接清算机构等；
——应建立服务对象风险识别标准和方法，识别和评估不同服务对象的风险状况；
——应开展持续的动态风险管理，如采取分渠道采集信息、加权测评、综合评价的方式，对服务对象的信用情况及对业务风险的持续管理能力定期开展审查与评估；
——应定期检查服务对象的风险评估报告，根据服务对象不同的风险等级，对其申请所开展业务的种类、范围进行区分和管理；
——应对服务对象接入设施的标准符合性进行核验，保证接入设施符合国家相关政策及标准要求。

9.2 TR 风险控制要求

TR风险控制要求如下：
——应面向用户提供欺诈防范咨询服务和紧急援助服务；
——应通过编写风险防范指引等材料，协同银行、非银行支付机构、支付转接清算机构等相关机构向用户或商户提供风险管理业务培训；
——信息采集的终端设备应具备相应安全防护措施。

10 安全要求

10.1 物理安全

应符合JR/T 0071—2012，6.2.1.1中的要求。

10.2 网络安全

应符合JR/T 0071—2012，6.2.1.2中的要求。

10.3 主机安全

应符合JR/T 0071—2012，6.2.1.3中的要求。

10.4 应用安全

10.4.1 身份鉴别

应符合JR/T 0071—2012，6.2.1.4中列项1)要求。

10.4.2 访问控制

应符合JR/T 0071—2012，6.2.1.4中列项2)要求。

10.4.3 安全审计

应符合JR/T 0071—2012，6.2.1.4中列项3)要求。

10.4.4 剩余信息保护

应符合JR/T 0071—2012，6.2.1.4中列项4)要求。

10.4.5 通信完整性

应符合JR/T 0071—2012，6.2.1.4中列项5)要求。

10.4.6 通信保密性

应符合 JR/T 0071—2012，6.2.1.4 中列项 6)要求。

10.4.7 抗抵赖

应符合 JR/T 0071—2012，6.2.1.4 中列项 7)要求。

10.4.8 应用容错

应符合JR/T 0071—2012，6.2.1.4中列项8)要求。

10.4.9 资源控制

应符合JR/T 0071—2012，6.2.1.4中列项9)要求。

10.4.10 会话安全

会话安全要求如下：

——会话标识应唯一，并具有随机性；

——会话过程中应维持认证状态，防止信息未经授权访问；

——会话结束后，应及时清除会话信息；

——应采取措施防止会话令牌在传输、存储过程中被窃取；

——应用审计日志应记录暴力破解会话令牌的事件。

10.4.11 常见攻击防范

常见攻击防范要求如下：

——应在服务器端对用户提交的数据进行有效性检查（如对提交的表单、参数等进行合法性判断和非法字符过滤等），或对输出进行安全处理；

——应进行代码审查，防范应用程序中不可信数据被解析为命令或查询语句等；

——应开发安全的接口，如通过避免语句的完全解释或采用参数化接口等方式实现；

——应采取有效措施防范服务器端的拒绝服务攻击；

——应对文件的上传和下载进行访问控制，避免执行恶意文件或未授权访问；

——数据库应使用存储过程或参数化查询，并严格定义数据库用户的角色和权限；

——应通过自动化工具（如弱点扫描工具、静态代码检测工具等）对应用程序进行检查；

——应使用安全控件、安全插件等措施以降低恶意软件窃取敏感信息的风险；

——应定期进行漏洞扫描和渗透性测试，并对已知漏洞及时进行修补。

10.4.12 WEB 页面安全

WEB页面安全要求如下：

——应提供登录防穷举的措施，如图片验证码等；

——登录应使用安全控件；

——应使用服务器证书，并在整个生命周期保障 Token 的安全；

——网站页面应采取防范 SQL 注入、Path 注入和 LDAP 注入等风险的措施；

——网站页面应采取防范跨站脚本攻击风险的措施；
——网站页面应采取防范源代码暴露的措施；
——应采取防范网站页面黑客挂马的机制和措施；
——应部署防篡改措施或设备；
——网站页面应提供防钓鱼网站的防伪信息验证。

10.4.13 客户端程序安全

客户端程序安全要求如下：
——移动终端客户端程序发布前应进行严格的代码安全测试，防止存在 SQL 注入、后门等漏洞；
——移动终端客户端程序应具有抗逆向分析、抗反汇编等安全性防护措施，防范攻击者对移动终端客户端程序的调试、分析和篡改；
——移动终端客户端程序应具备完整性校验功能防止程序文件被非授权篡改；
——移动客户端程序安装及卸载功能应满足安全需求；
——应对客户端应用软件敏感数据留存情况进行检查，防止客户敏感信息泄露；
——应对客户端配置文件进行保护，严格控制对其的访问、修改等操作；
——用户口令等敏感信息在本地不应明文存储；
——禁止明文显示密码，应使用相同位数的同一特殊字符（例如*或#）代替；
——应建立客户端程序的安全检测机制，每年至少全面检测一次，通过程序升级等方式及时修补漏洞；
——客户端应具备客户端环境安全检测能力，在检测到运行环境处于 ROOT 或已越狱等非安全环境时，向客户进行必要的安全警示，必要时可停止运行客户端；
——客户端对用户登录应采取限定连续登录失败次数等措施；
——当客户端检测到移动终端交易出现异常时应向用户提示出错信息；
——客户端在使用过身份认证、交易等敏感信息后，应及时清除敏感数据；
——客户端宜提供数据有效性校验功能，保证通过人机接口或通信接口输入的数据格式或长度等信息符合系统设定要求，如输入的资金金额、账户等信息应不含特殊字符；
——客户端宜具备页面回退清除敏感信息的机制；
——用户输入敏感数据时，宜采取安全措施保证敏感数据不被移动终端的其他设备或程序非授权获取；
——用户输入敏感数据时，宜采取防篡改机制保证数据不被移动终端的其他设备或程序篡改。

10.4.14 用户与 TR 系统间安全要求

用户与TR系统间安全要求如下：
——用户通过互联网连接 TR 传输数据时，应采用数字证书保证数据的机密性、完整性和不可抵赖性。应使用足够强度的加密算法和安全协议保护客户端与服务器之间的连接；
——采集账户敏感信息时，TR 应使用符合要求的安全控件对敏感信息进行保护；
——TR 不得留存账户敏感信息。TR 存储 Token 时，应对 Token 实施有效的安全保护。

10.4.15 TR 与 TSP 系统间安全要求

TR与TSP系统间安全要求如下：
——所有 TR 与 TSP 系统之间的报文中的敏感信息应加密传输；
——TR 通过互联网连接 TSP 传输数据时，应采用数字证书保证数据的机密性、完整性和不可抵赖性。应使用安全算法和安全协议保护客户端与服务器之间的连接。

10.5 数据安全

10.5.1 数据完整性

应符合JR/T 0071—2012，6.2.1.5中列项1)要求。

10.5.2 数据保密性

应符合 JR/T 0071—2012，6.2.1.5 中列项 2)要求。

在申请 Token 的过程中对于敏感数据要进行加密处理。申请过程包括用户信息采集、信息传递、信息存储。敏感数据主要包括 PA 及验证要素。

10.5.3 备份和恢复

应符合JR/T 0071—2012，6.2.1.5中列项3)要求。

10.5.4 报文安全

报文安全要求如下：

——应对报文完整性进行验证；

——应保证报文保密性。

10.5.5 安全算法

应使用经国家密码管理机构认可的商用密码产品。

10.6 运维安全

10.6.1 环境管理

应符合 JR/T 0071—2012，6.2.2.5 中列项 1)要求。

10.6.2 资产管理

应符合JR/T 0071—2012，6.2.2.5中列项2)要求。

10.6.3 介质管理

应符合JR/T 0071—2012，6.2.2.5中列项3)要求。

10.6.4 设备管理

应符合JR/T 0071—2012，6.2.2.5中列项4)要求。

10.6.5 监控管理

应符合JR/T 0071—2012，6.2.2.5中列项5)要求。

10.6.6 网络安全管理

应符合JR/T 0071—2012，6.2.2.5中列项6)要求。

应至少每半年对网络系统进行一次漏洞扫描，并保存扫描记录。

应对扫描发现的漏洞进行处理。

10.6.7 系统安全管理

应符合JR/T 0071—2012，6.2.2.5中列项7)要求。

10.6.8 恶意代码防范管理

应符合JR/T 0071—2012，6.2.2.5中列项8)要求。

10.6.9 密码管理

应符合JR/T 0071—2012，6.2.2.5中列项9)要求。

10.6.10 变更管理

应符合JR/T 0071—2012，6.2.2.5中列项10)要求。

10.6.11 备份与恢复管理

应符合JR/T 0071—2012，6.2.2.5中列项11)要求。

10.6.12 安全事件处置

应符合JR/T 0071—2012，6.2.2.5中列项12)要求。

10.6.13 应急预案管理

应符合JR/T 0071—2012，6.2.2.5中列项13)要求。

10.7 业务连续性

10.7.1 业务连续性需求分析

业务连续性需求分析要求如下：

——应进行业务中断影响分析和业务连续性计划；

——应具备灾难恢复时间目标和恢复点目标。

10.7.2 业务连续性技术环境

业务连续性技术环境要求如下：

——应具备应用级备份机房；

——主机房应具备网络通信双链路，双链路应来自不同运营商；

——主机房应具有应用级备份设施，保证系统的高可用性；

——应使用高可靠的存储设备；

——应具备远程备份数据库。

10.8 日常维护

日常维护要求如下：

——应每年进行业务连续性演练；

——应定期进行业务连续性培训并具有培训记录。

10.9 性能可靠性

10.9.1 TSP 系统性能可靠性要求

TSP性能可靠性要求如下：

——TSP 系统应满足未来三年业务运行的性能需求。
——系统应支持业务的多用户并发操作；在规定的硬件环境条件和给定的业务压力下，系统应满足性能需求和压力解除后系统自恢复能力；系统性能极限应满足业务需求。
——应结合典型交易、复杂业务流程、频繁的用户操作、大数据量处理等原则，选取测试业务点进行检测。

10.9.2 TR 系统性能可靠性要求

TR性能可靠性要求如下：
——TR 系统应满足未来三年业务运行的性能需求。
——系统应支持业务的多用户并发操作；在规定的硬件环境条件和给定的业务压力下，系统应满足性能需求和压力解除后系统自恢复能力；系统性能极限应满足业务需求。
——应结合典型交易、复杂业务流程、频繁的用户操作、大数据量处理等原则，选取测试业务点进行检测。

10.10 管理安全

10.10.1 管理制度

应符合JR/T 0071—2012，6.2.2.1中列项1)要求。

10.10.2 组织机构

组织机构要求如下：
——应建立信息安全管理架构，设置专门的系统研发、测试、运行维护、信息安全、风险控制等部门或团队；
——应明确各部门的信息安全职责，并详细定义部门人员配置和岗位职责；
——应建立风险管理架构，相关人员应详细了解本单位研发、运行及管理机构职责设置。

10.10.3 岗位设置

应符合JR/T 0071—2012，6.2.2.2中列项1)要求。

10.10.4 人员配备

应符合JR/T 0071—2012，6.2.2.2中列项2)要求。

10.10.5 人员和文档安全管理

应符合JR/T 0071—2012，6.2.2.3中的要求。
应建立文档管理制度，文档资料按密级或敏感程度进行登记、分类并由专人保管，重要文档资料的使用、外借或销毁应经过审批流程并进行记录。

附 录 A
（资料性附录）
交易要素

A.1 标记申请要素

标记申请要素参见表A.1。

表A.1 标记申请要素

要素定义	属性	输入	输出	是否为域控要素	备注
标记请求方 ID Token Requestor ID	n11	M			TR 的唯一识别码，由 TSP 为 TR 分配。
账号的长度 PA Length	n3	M			PA 的长度。
账号 PA	an..128	M			作为标记化对象的支付账号。 对于银行卡卡号长度不超过 19 位。
账号发行方 PA Issuer	an15	C			用于表示发行支付账号的机构，对于账号取值中不能隐含发行机构归属的，应提供该信息。
账号的有效期 PA Expiry Date	n4	C			表示支付账号有效期。
标记存储位置 Token Location	n2	C		是	支付标记的存储位置，宜采用以下取值： ——01：远程存储，例如大商户的服务器； ——02：SE（安全芯片）存储，例如芯片，移动设备中的 SE； ——03：本地安全环境存储，例如 TEE（可信执行环境）； ——04：远程安全环境存储：如云 SE，即 HCE（基于主机的模拟卡）； ——05：本地软件环境存储，例如移动设备中的客户端软件； ——06-99：保留使用。
账户验证结果 Account Verification Results	n2	O			表示 TR 关于商户侧账户信息验证的结果。

表A.1 标记申请要素（续）

要素定义	属性	输入	输出	是否为域控要素	备注
账户验证参考数据 Account Verification Reference	an..99	M			用于辅助 TSP 进行账户验证的信息。
标记欺诈风险评估值 Token Requestor Risk Score	n4	O			TR 提供的风险评估值。
用户数据 Cardholder Data	an..9999	C			用于实现标记保护的 ID&V 方法的用户数据。 对于 TSP 向 PA 发行方提交 ID&V 请求时，应传递。 对于由 TR 向 PA 发行方提交 ID&V 请求的情况，可不送。
设备信息 Device Information	an99	O			设备信息用于识别存储支付标记的专有设备，如安全单元（SE）的 ID 或者设备特征如 MAC 地址、操作系统版本号、语言等。
使用次数 Usage Time	n4	M		是	标记的最大使用次数，取值范围 0000-9999。取值 0000 表示无次数限制。
交易渠道权限 Transaction Chanel	n7	M		是	表示标记允许受理的交易渠道，渠道权限位图，0-不支持，1-支持。 ——第 1 位：ATM； ——第 2 位：手机； ——第 3 位：个人电脑； ——第 4 位：多媒体终端； ——第 5 位：固话终端； ——第 6 位：POS； ——第 7 位：其他。
商户范围 Merchant Range	n1	M		是	表示标记受理商户范围，由 TR 设定的该 Token 能在一个或多个商户中使用。 0-单商户受理； 1-多商户受理。

表A.1　标记申请要素（续）

要素定义	属性	输入	输出	是否为域控要素	备注
金额限制 Amount Limit	n12	M		是	表示标记在支付交易中的最大交易限额，支付环节 Token 交易限额与 PA 的交易限额中的较小值作为实际生效的交易限额。 TSP 对每个 TR 应设置金额域控制参数。TR 的整体金额限制参数值由 TR 向 TSP 申请注册时与 TSP 约定。 TSP 在生成 Token 时，对 TR 域控参数中的交易限额和申请 Token 时 TR 上送的客户申请的金额进行比对，取其中的最小值来赋值 Token 的交易限额。
标记申请返回状态 Request Status	n1		M		表示标记申请成功或失败。
失败原因 Reason Code	an99		C		失败原因信息。
标记 Payment Token	n13..34		C		如申请成功，由 TSP 生成。
标记有效期 Token Expiry Date	n4		C	是	如申请成功，由 TSP 生成。
账号识别提示信息 PA Suffix	VAR		C		如申请成功，由 TSP 生成，返回给 TR，TR 可提供给用户，以提示用户 Token 关联的具体账号。 应依据 PA 发行方脱敏规则返回脱敏后的账号。

A.2 标记交易要素

标记交易要素参见表A.2。

表A.2 Token 交易要素

要素名称	属性	输入	输出	是否为域控要素	备注
标记请求方 ID Token Requestor ID	n11	C			当去标记化申请方可用时一定包含该参数。 该值可用来唯一标识 TR 与标记域的配对。
标记长度 Token Length	n2	M			支付标记的长度。
标记 Payment Token	n13..34	M			发行的支付标记。
标记的有效期 Token Expiry Date	n4	M		是	标记有效期。
请求数据长度 Request Data Length	n3	M			TSP 要求的交易数据的长度。
请求数据 Request Data	ans	O			TSP 要求的交易数据。
去标记化返回状态 Request Status	n1		R		表示去标记化的成功或失败。
失败原因的长度 Reason Code Length	n2		R		失败原因信息长度。
失败原因 Reason Code	an99		C		失败原因信息。
账号的长度 PA Length	n3		C		去标记化成功，返回该字段。
支付账号 PA	an..128		C		去标记化成功，返回该字段。
账号的有效期 PA Expiry Date	n4		C		去标记化成功，返回该字段。
应答数据长度 Response Data Length	n3		R		TSP 返回的交易数据的长度。
应答数据 Response Data	ans		O		TSP 返回的交易数据。

A.3 TR注册要素

TR注册要素参见表A.3。

表A.3 TR 注册信息表

注册信息	是否为域控要素	备注
主体名称		申请成为 TR 的实体的名称。
组织机构代码证		申请成为 TR 的实体的组织机构代码证。
税务登记证		申请成为 TR 的实体的税务登记证。
营业执照编号		申请成为 TR 的实体的营业执照编号。
法人代表		申请成为 TR 的实体的法人代表姓名。
法人代表身份证号		申请成为 TR 的实体的法人代表身份证号。
结算账户名称		申请成为 TR 的实体的结算账户名称。
结算账号		申请成为 TR 的实体的结算账户号。
结算账户开户行行号		申请成为 TR 的实体的结算账户开户行行号。
结算账户开户行名称		申请成为 TR 的实体的结算账户开户行名称。
使用次数	是	控制该 TR 申请的 Token 的有效使用次数。
使用时间	是	控制该 TR 申请的 Token 的有效使用时间。
存储位置	是	控制该 TR 申请的 Token 存储位置。
交易渠道	是	控制该 TR 申请的 Token 所允许的交易渠道。
交易商户	是	控制该 TR 申请的 Token 所允许的具体商户。
读取方式	是	控制该 TR 申请的 Token 在受理环节执行有卡交易还是无卡交易。
是否跨商户受理	是	控制该 TR 申请的 Token 是否可以跨商户受理。

表A.3 TR注册信息表（续）

注册信息	是否为域控要素	备注
交易金额限制	是	控制该TR申请的所有Token的交易限额。
Token使用场景		场景包括但不限于： ——二维码支付； ——大商户支付； ——数字钱包； ——近场支付。

参 考 文 献

[1] EMVCo payment tokenisation specification technical framework 1.0