本资料来源于中国支付网 www.paynews.net

ICS 35.240.40
A11

JR

中 华 人 民 共 和 国 金 融 行 业 标 准

JR/T XXXXX—XXXX

中国金融移动支付　应用基础
第 1 部分：术语

China financial payment--Application basis
Part 1: Terminology

（报批稿）

（本稿完成日期：2012 年 10 月 22 日）

XXXX－XX－XX 发布　　XXXX－XX－XX 实施

中国人民银行　　发 布

本资料来源于中国支付网 www.paynews.net

目　　次

前言 II
引言 III
1　范围 1
2　规范性引用文件 1
3　术语 1
4　缩略语 7
附录 A（资料性附录）　中文索引 8
附录 B（资料性附录）　英文索引 10
参考文献 12

本资料来源于中国支付网 www.paynews.net

前　　言

《中国金融移动支付　应用基础》标准由以下4部分构成：

——第1部分：术语；

——第2部分：机构代码；

——第3部分：支付应用标识符；

——第4部分：支付账户介质识别码；

本部分为该标准的第1部分。

本部分按照GB/T 1.1-2009给出的规则起草。

本部分由中国人民银行提出。

本部分由全国金融标准化技术委员会（SAC/TC180）归口。

本部分负责起草单位：。

本部分参加起草单位：。

本部分主要起草人：。

本资料来源于中国支付网 www.paynews.net

引　　言

移动支付是一种涉及多个行业的新兴支付方式，近年来在国内外迅速发展且发展前景及潜力巨大。然而，目前国内尚缺乏系统的移动支付术语规范，相关定义不统一，为了系统全面地规范移动支付的相关内容，特制定此规范。

本部分明确了移动支付领域涉及到的术语及其定义，为移动支付知识的普及奠定了基础，为移动支付产业的各参与方在新技术和新应用方面的合作提供了参考和依据，为移动支付更好地服务国民经济和社会发展给予了支持。

本资料来源于中国支付网 www.paynews.net

中国金融移动支付　应用基础　第1部分：术语

1　范围

本部分是移动支付产业中的基础性标准。

本部分规范了移动支付标准领域的用词，统一表达，并为移动支付其他各项标准的编制提供参照。附录A和附录B分别给出了移动支付术语的中文和英文索引。

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。

GB/T 16649 识别卡 带触点的集成电路卡

GB/T 22186-2008 具有中央处理器的集成电路（IC）卡芯片安全技术要求（评估保证级4增强级）

GB/T 25069-2010 信息安全技术 术语

JR/T 0025-2010 中国金融集成电路（IC）卡规范

JR/T 0061-2011 银行卡名词术语

3　术语

3.1

移动终端　mobile device

具有移动通讯能力的终端设备，包括手机、PDA等，在本规范中主要指手机。

3.2

受理终端（POI）　point of interaction (POI)

参与移动支付交易的受理机具，包括POS、ATM等。

3.3

分体终端 separated mobile payment terminal

可以与外部设备（如手机，PDA等）相连，借助相关设备完成移动支付交易。分体终端按照适用的环境及功能不同，可以分为个人类设备和商户类设备。

3.4

移动支付　mobile payment

允许用户使用移动终端对所消费的商品或服务进行账务支付的一种服务方式，主要分为近场支付和远程支付两种。

本资料来源于中国支付网 www.paynews.net

3.5

近场支付 proximity payment

移动终端通过实体受理终端在交易现场以联机或脱机方式完成交易处理的支付方式。

3.6

远程支付 remote payment

移动终端通过无线通信网络接入，直接与后台服务器进行交互完成交易处理的支付方式。

3.7

短信支付 SMS payment

预先建立手机号码与支付账户的绑定关系，通过短信进行支付的业务。

3.8

支付账户 payment account

非金融支付机构根据客户申请,为客户开立的具有记录客户人民币资金交易和资金余额功能的电子账簿。

3.9

支付内容平台 content provider platform

提供商品或服务内容的平台。

3.10

应用 application

在SE上安装后处于可选择状态的可执行模块的实例。

3.11

安全单元（SE） secure element (SE)

在移动支付中负责交易关键数据的安全存储和运算功能的部件。

3.12

空中圈存 remote load

用户在移动终端上发起指令,通过无线通信网络将其在账户管理系统上的资金划转到安全载体上的脱机账户中。

3.13

电子现金 electronic cash

基于借记/贷记应用实现的小额支付功能。

3.14

远程支付系统 remote payment system

为远程支付提供移动终端接入、交易信息及结算数据的处理等功能的系统。

本资料来源于中国支付网 www.paynews.net

3.15

收单系统 acquiring system

为近场支付提供受理终端接入、交易信息及结算数据的处理等功能的系统。

3.16

账户管理系统 account management system

为银行账户或支付账户提供资金管理、结算等业务的系统。

3.17

转接清算系统 switch and clearing system

实现跨机构支付的业务转接、清算和结算功能的系统。

3.18

卡片操作系统（COS） chip operating system (COS)

主要用于接收和处理外界(如手机或者读卡器)发给卡片的各种信息，执行外界发送的各种指令(如鉴权运算等），管理卡内的存储器空间，向外界回送应答信息等的专用系统软件。

3.19

密钥管理系统（KMS） key management system (KMS)

用来对密钥的生成、加载、存储、备份、分发、更新、归档、销毁等生命周期各环节进行管理的系统。

3.20

可信服务管理（TSM） trusted service management (TSM)

由可信第三方提供的载体生命周期管理、应用生命周期管理和应用管理等服务。

3.21

公共服务平台 public service platform

移动支付参与各方认可的可信第三方系统，提供机构注册接入、应用注册、跨机构交互转接、SE可信管理、SE开放共享功能、应用共享等功能。

3.22

证书认证机构（CA） certificate authority (CA)

证书的签发机构，是负责签发证书、认证证书、管理已颁发证书的机构，负责制定政策和具体步骤来验证、识别用户身份，并对用户证书进行签名，以确保证书持有者的身份和公钥的拥有权，也称认证中心。

3.23

应用提供方 application provider

提供支付应用的主体。

3.24

安全单元发行方 SE issuer

本资料来源于中国支付网 www.paynews.net

为用户提供安全单元发行服务的主体。

3.25

受理方 acquirer

受理交易的主体，主要负责交易信息的产生和转接以及结算数据的收集、整理和提交等。

3.26

TSM 运营方 TSM operator

运营TSM的主体。

3.27

账户管理机构 account management institution

运营账户管理系统的机构，包括商业银行、非金融支付机构等。

3.28

委托管理 delegated management

由认证后的应用提供方来执行的、预先授权的对SE内容进行改变的行动。

3.29

授权管理者 controlling authority

借助强制性的数据鉴别模式的确认，拥有对SE内容进行管理控制权限的角色。

3.30

客户端 client software

在移动终端上实现金融支付功能的应用软件。

3.31

智能 SD 卡 smart SD card

内嵌了安全运算单元和安全存储模块的SD卡。

3.32

支付控件 payment controller

保证支付过程安全的控件。

3.33

应用协议数据单元（APDU） application protocol data unit (APDU)

读卡器和SE之间的标准通信消息协议。

3.34

非接触前端（CLF） contactless front-end (CLF)

实现近场非接触通讯功能的控制模块。

本资料来源于中国支付网 www.paynews.net

3.35

冲突 collision

在同一时间周期内，在同一接近式耦合设备（PCD）的工作场中，有两个或两个以上的SE进行数据传输，使得PCD不能辨别数据是从哪一个SE发出的。

3.36

防冲突机制 anti-collision mechanism

保证PCD检测到多个SE时，能够对每个SE进行正常处理的机制。

3.37

动态口令（OTP） one time password (OTP)

也称一次性密码，它指在认证过程中只使用一次，下次认证时则更换使用另一个口令，每个密码只使用一次。动态口令身份认证目前主要有基于时间同步机制、基于事件同步机制和基于挑战/应答（异步）机制三种技术模式。

3.38

个人标识码（PIN） personal identification number (PIN)

即个人密码，是在联机交易中识别持卡人身份合法性的数据信息，在计算机和网络系统中的任何环节都不允许PIN以明文的方式出现。

3.39

脱机PIN验证 offline PIN verification

一种持卡人身份的验证方式，该方式通过终端和SE的交互来比较持卡人输入的PIN与SE芯片内存储的PIN是否一致来验证持卡人身份。

3.40

联机PIN验证 online PIN verification

一种持卡人身份的验证方式，该方式将加密后的PIN值通过授权请求报文发送至发卡行，通过比较报文中PIN值与发卡行PIN值是否一致来验证持卡人身份。

3.41

报文鉴别码（MAC） message authentication code （MAC）

用来完成消息来源正确性鉴别，防止数据被篡改或非法用户窃入的数据。

3.42

单线传输协议（SWP） single wire protocol (SWP)

非接触前端和安全单元之间通过一根信号线通讯的接口协议。

3.43

双因子认证（2FA） two-factor authentication (2FA)

除静态密码外，采用动态密码、数字证书等技术，通过双重认证的方式加强身份管理的认证方式。

本资料来源于中国支付网 www.paynews.net

3.44

短信动态密码 SMS dynamic code

又称短信密码，是后台系统以手机短信形式发送到用户绑定手机上的随机数，用户通过回复该随机数进行身份认证。

3.45

数字证书 digital certificate

由认证中心签名的不可伪造的某个实体的公钥信息。

3.46

数字签名 digital signature

一种特殊的加密算法，数据接收者能够借此确认数据的来源和完整性，避免数据被第三方篡改，数据发送者也可以借此确保数据不会被接收者篡改。

3.47

安全域 security domain

负责对某个SE外实体（例如SE发行方、应用提供方、授权管理者）的管理、安全、通信需求进行支持的SE内实体。

3.48

主安全域（ISD） issuer security domain (ISD)

负责对SE管理者(通常是SE发行方)的管理、安全、通信需求进行支持的SE上首要实体，也称发行方安全域。

3.49

辅助安全域（SSD） supplementary security domain (SSD)

SE发行方安全域之外的其他安全域。

3.50

令牌 token

由授权方出具的用来作为一个委托管理操作已经被授权进行的证据。

3.51

支付应用标识符（PAID） payment application identifier (PAID)

移动支付中唯一标识SE中应用实例的代码。

3.52

注册应用提供方标识符（RID） registered application provider identifier (RID)

所有移动支付应用共用的唯一标识。

3.53

机构代码 institution identification code

本资料来源于中国支付网 www.paynews.net

在移动支付交易转接清算以及接入公共服务平台时，用于标识支付机构或TSM运营方的唯一代码。

3.54

应用类型代码 application type code

移动支付中标识具有相同特点的一类应用的代码。

3.55

专有应用标识符扩展（PIX） proprietary application identifier extension (PIX)

支付应用标识符中对同一RID下不同的专有应用进行标识的代码。

3.56

支付账户介质识别码（PAMID） payment account media identifier (PAMID)

唯一标识支付账户介质的代码。

3.57

安全载体 secure media

承载安全单元的介质。

4 缩略语

表1 缩略语说明

AP	Application Processor	应用处理芯片
APDU	Application Protocol Data Unit	应用协议数据单元
BP	Baseband Processor	基带处理芯片
CA	Certificate Authority	认证中心
CLF	Contactless Front-end	非接通讯前端
COS	Chip Operation System	卡片操作系统
MAC	Message Authentication Code	报文鉴别码
NFC	Near Field Communication	近场通讯
PAID	Payment Application Identifier	支付应用标识符
PAN	Primary Account Number	主账号
PCD	Proximity Coupling Device	读卡器
PICC	Proximity Card	近场耦合卡
PIN	Personal Identification Number	个人标识码
PKI	Public Key Infrastructure	公钥基础设施
SSL	Secure Sockets Layer	安全套接层
STK	SIM Toolkit	SIM卡工具包
SWP	Single Wire Protocol	单线传输协议
TMK	Terminal Master Key	终端主密钥
TSM	Trusted Service Management	可信服务管理
WK	Working Key	工作密钥（数据密钥）
2FA	Two Factors Authentication	双因子认证

本资料来源于中国支付网 www.paynews.net

本资料来源于中国支付网 www.paynews.net

附 录 A
（资料性附录）
中文索引

	A	
安全单元（SE）	secure element(SE)	3.11
安全单元发行方	SE issuer	3.24
安全域	security domain	3.47
安全载体	secure madia	3.57
	B	
报文鉴别码（MAC）	message authentication code(MAC)	3.41
	C	
冲突	collision	3.35
	D	
短信支付	SMS payment	3.7
电子现金	electronic cash	3.13
动态口令（OTP）	one time password(OTP)	3.37
单线传输协议（SWP）	single wire protocol(SWP)	3.42
短信动态密码	SMS dynamic code	3.44
	F	
分体终端	separated mobile payment interaction	3.3
非接触前端（CLF）	contactless front-end(CLF)	3.34
防冲突机制	anti-collision mechanism	3.36
辅助安全域（SSD）	supplementary security domain(SSD)	3.49
	G	
个人标识码（PIN）	personal identification number(PIN)	3.38
	J	
近场支付	proximity payment	3.5
机构代码	institution identification code	3.53
	K	
空中圈存	remote load	3.12
卡片操作系统（COS）	chip operating system(COS)	3.18
可信服务管理（TSM）	trusted service management(TSM)	3.20
客户端	client software	3.30
	L	
联机 PIN 验证	online PIN verification	3.40
令牌	token	3.50

本资料来源于中国支付网 www.paynews.net

	M	
密钥管理系统（KMS）	key management system(KMS)	3.19
	S	
受理终端（POI）	point of interaction(POI)	3.2
收单系统	acquiring system	3.15
受理方	Acquirer	3.25
授权管理者	controlling authority	3.29
双因子认证（2FA）	two-factor authentication(2FA)	3.43
数字证书	digital certificate	3.45
数字签名	digital signature	3.46
	T	
公共服务平台	public service platform	3.21
脱机 PIN 验证	offline PIN verification	3.39
	W	
委托管理	delegated management	3.28
	Y	
移动终端	mobile device	3.1
移动支付	mobile payment	3.4
远程支付	remote payment	3.6
应用	Application	3.10
远程支付系统	remote payment system	3.14
应用提供方	application provider	3.23
应用协议数据单元（APDU）	application protocol data unit(APDU)	3.33
应用类型代码	application type code	3.54
	Z	
支付账户	payment account	3.8
支付应用标识符（PAID）	payment application identifier(PAID)	3.51
支付内容平台	content provider platform	3.9
支付账户介质识别码（PAMID）	payment account media identifier(PAMID)	3.56
账户管理系统	account management system	3.16
转接清算系统	switch and clearing system	3.17
证书认证机构（CA）	certificate authority(CA)	3.22
账户管理机构	account management institution	3.27
智能 SD 卡	smart SD card	3.31
支付控件	payment controller	3.32
主安全域（ISD）	issuer security domain(ISD)	3.48
注册应用提供方标识符（RID）	registered application provider identifier(RID)	3.52
专有应用标识符扩展（PIX）	proprietary application identifier extension(PIX)	3.55

本资料来源于中国支付网 www.paynews.net

附 录 B
（资料性附录）
英文索引

	A	
Application	应用	3.10
acquiring system	收单系统	3.15
account management system	账户管理系统	3.16
application provider	应用提供方	3.23
Acquirer	受理方	3.25
account management institution	账户管理机构	3.27
application protocol data unit（APDU）	应用协议数据单元(APDU)	3.33
anti-collision mechanism	防冲突机制	3.36
application type code	应用类型代码	3.54
	C	
content provider platform	支付内容平台	3.9
chip operating system（COS）	卡片操作系统(COS)	3.18
certificate authority（CA）	证书认证机构(CA)	3.22
controlling authority	授权管理者	3.29
client software	客户端	3.30
contactless front-end（CLF）	非接触前端(CLF)	3.34
collision	冲突	3.35
	D	
delegated management	委托管理	3.28
digital certificate	数字证书	3.45
digital signature	数字签名	3.46
	E	
electronic cash	电子现金	3.13
	I	
issuer security domain（ISD）	主安全域(ISD)	3.48
institution identification code	机构代码	3.53
	K	
key management system（KMS）	密钥管理系统(KMS)	3.19
	M	
mobile device	移动终端	3.1
mobile payment	移动支付	3.4
message authentication code（MAC）	报文鉴别码(MAC)	3.41
	O	

本资料来源于中国支付网 www.paynews.net

one time password（OTP）	动态口令(OTP)	3.37
offline PIN verification	脱机 PIN 验证	3.39
online PIN verification	联机 PIN 验证	3.40
	P	
point of interaction（POI）	受理终端(POI)	3.2
proximity payment	近场支付	3.5
payment account	支付账户	3.8
payment application identifier（PAID）	支付应用标识符(PAID)	3.51
payment controller	支付控件	3.32
personal identification number（PIN）	个人标识码(PIN)	3.38
proprietary application identifier extension（PIX）	专有应用标识符扩展(PIX)	3.55
payment account media identifier（PAMID）	支付账户介质识别码(PAMID)	3.56
	R	
remote payment	远程支付	3.6
remote load	空中圈存	3.12
remote payment system	远程支付系统	3.14
registered application provider identifier（RID）	注册应用提供方标识符(RID)	3.52
	S	
separated mobile payment terminal	分体终端	3.3
SMS payment	短信支付	3.7
secure element（SE）	安全单元(SE)	3.11
switch and clearing system	转接清算系统	3.17
SE issuer	安全单元发行方	3.24
smart SD card	智能 SD 卡	3.31
single wire protocol（SWP）	单线传输协议(SWP)	3.42
SMS dynamic code	短信动态密码	3.44
security domain	安全域	3.47
supplementary security domain（SSD）	辅助安全域(SSD)	3.49
secure media	安全载体	3.57
	T	
trusted service management（TSM）	可信服务管理(TSM)	3.20
TSM operator	TSM 运营方	3.26
two-factor authentication（2FA）	双因子认证(2FA)	3.43
token	令牌	3.50
	U	
public service platform	公共服务平台	3.21

本资料来源于中国支付网 www.paynews.net

本资料来源于中国支付网 www.paynews.net

参 考 文 献

[1] ISO/IEC 14443-1 Identification cards - Contactless integrated circuit(s)cards - Proximity cards Part 1: Physical characteristics

[2] ISO/IEC 14443-2 Identification cards - Contactless integrated circuit(s) cards-Proximity cards Part 2: Radio frequency power and signal interface

[3] ISO/IEC 14443-3 Identification cards - Contactless integrated circuit(s) cards-Proximity cards Part 3: Initialization and anticollision

[4] ISO/IEC 14443-4 Identification cards - Contactless integrated circuit(s) cards-Proximity cards Part 4: Transmission protocol

[5] ETSI TS102 613 Smart Cards: UICC - Contactless Front-end (CLF) Interface; Part 1: Physical and data link layer characteristics

[6] ETSI TS102 622 Smart Cards; UICC - Contactless Front-end (CLF) Interface; Host Controller Interface (HCI)

[7] SWP Single Wire Protocol

[8] SD Card Specifications

[9] Global Platform Card Specfication V2.1.1