支付宝离线二维码技术规范

——蚂蚁金服创新支付技术部

文档修订记录

编号	文档版本	修订章节	修订原因	修订日期	修订人	确认人
1						
2						
3						
4						
5						
6						
7						
8						
9						

目录

1. 受众

本技术规范主要针对已应用或者准备应用支付宝离线二维码技术标准的合作伙伴，以便在统一的技术规范指导下进行商务合作和技术研发。

本技术规范受众包括对支付宝离线二维码技术感兴趣的各类合作伙伴，特别是手机厂商，POS 终端制造商、系统集成商、票卡发行商、应用开发商等。

本技术规范为支付宝应用和倡导的离线二维码开放技术标准，合作伙伴可根据实际情况应用本技术规范。

2. 参考规范

表格 1 参考规范

标准 / 规范	描述
ISO/IEC 14443-3:2001	Identification cards - Contactless integrated circuit(s) cards -Proximity cards - Part 3: Initialization and anticollision
ISO/IEC 14443-4:2001	Identification cards - Contactless integrated circuit(s) cards -Proximity cards - Part 4: Transmission protocol
JR/T 0025 PBOC 3.0	《中国金融集成电路（IC）卡规范 3.0》
EMV4.3	EMV Integrated Circuit Card Specifications for Payment Systems version 4.3
GB 2312	信息交换用汉字编码字符集・基本集

3. 术语和定义

表格 2 术语和定义

术语	定义
手机客户端	这里特指安装在手机上的应用本规范二维码应用的软件。
二维码票卡	特指通过二维码为载体发行的电子票卡，主要在形态上区别于实体票卡
票卡二维码	特指二维码票卡产生的二维码图案
二维码发行机构	特指发行离线二维码机构
票卡发行机构	特指发行二维码票卡的机构
公私密钥对	非对称密钥中的公钥和私钥
私钥	Private Key，非对称密钥对中，非公开的密钥
公钥	Public Key，非对称密钥对中，公开的密钥
受理终端	Terminal，这里指能支持识别和受理本规范二维码的终端设备
二维码受理记录	指受理终端受理票卡二维码后根据本规范生成的记录数据

4. 符号和缩略语

下列符号和缩略语表示适用于本规范。

表格 3 符号和缩略语

缩写	含义
ECDSA	elliptic curve digital signature algorithm 椭圆曲线数字签名算法
NFC	Near Field Communication 近场通讯
Hash	哈希或者散列
HMAC	Hash-based Message Authentication Code 密钥相关的哈希运算消息认证码
https	Hyper Text Transfer Protocol over Secure Socket Layer 以安全为目标的http通道
KMI	Key Management Infrastructure 密钥管理基础设施
MD5	Message Digest Algorithm MD5 消息摘要算法第五版
N/A	Not applicable 不适用
ID	Identification 身份编码
pos	Point of Sale 销售终端
posid	POS终端唯一编码
CPU	Central Processing Unit 中央处理单元
TEE	Trusted execution environment 可信运行环境

5. 系统描述

5.1. 涉众及关系

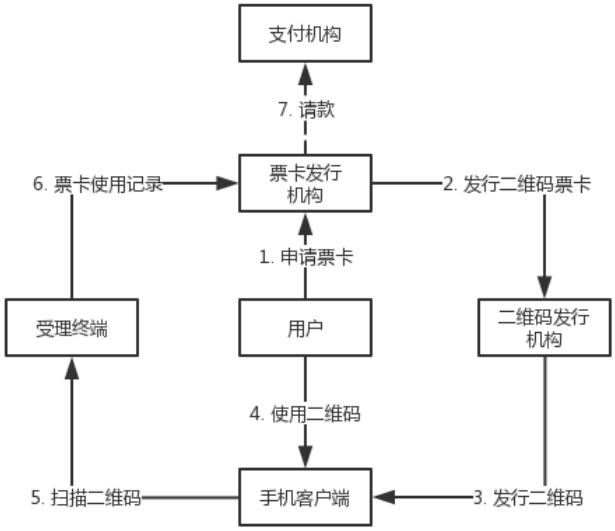

图 1 涉众及关系

- **票卡发行机构**：二维码票卡发行机构，向使用二维码票卡业务的用户发行二维码票卡，例如公交卡、校园卡、市民卡等发卡机构；票卡发行机构负责发行、运营和管理用户票卡；
- **二维码发行机构**：为二维码票卡发行二维码，可以是票卡发行机构本身，也可以是用户、票卡发行机构共同信任的可信第三方，例如支付宝、银联等支付机构；二维码发行机构负责认证用户身份，进行二维码的发行和管理，确保二维码的安全性；
- **用户**：使用票卡二维码业务的用户，通常为二维码发行机构注册用户；
- **手机客户端**：用户通过手机客户端使用二维码票卡业务，手机客户端生成票卡二维码，并由受理终端扫描识别；
- **受理终端**：受理票卡二维码的终端设备，扫描识别用户手机客户端的票卡二维码，验证用户二维码票卡有效性，进行联机/脱机交易，例如公交车刷卡终端等；
- **支付机构**：用户使用票卡二维码在受理终端上进行消费，票卡发行机构向对应的支付机构请款；支付机构可以是银行、第三方支付机构等，也可以是票卡发行机构本身；支付机构负责提供联机/脱机支付功能，确保资金账户安全；

5.2. 工作原理

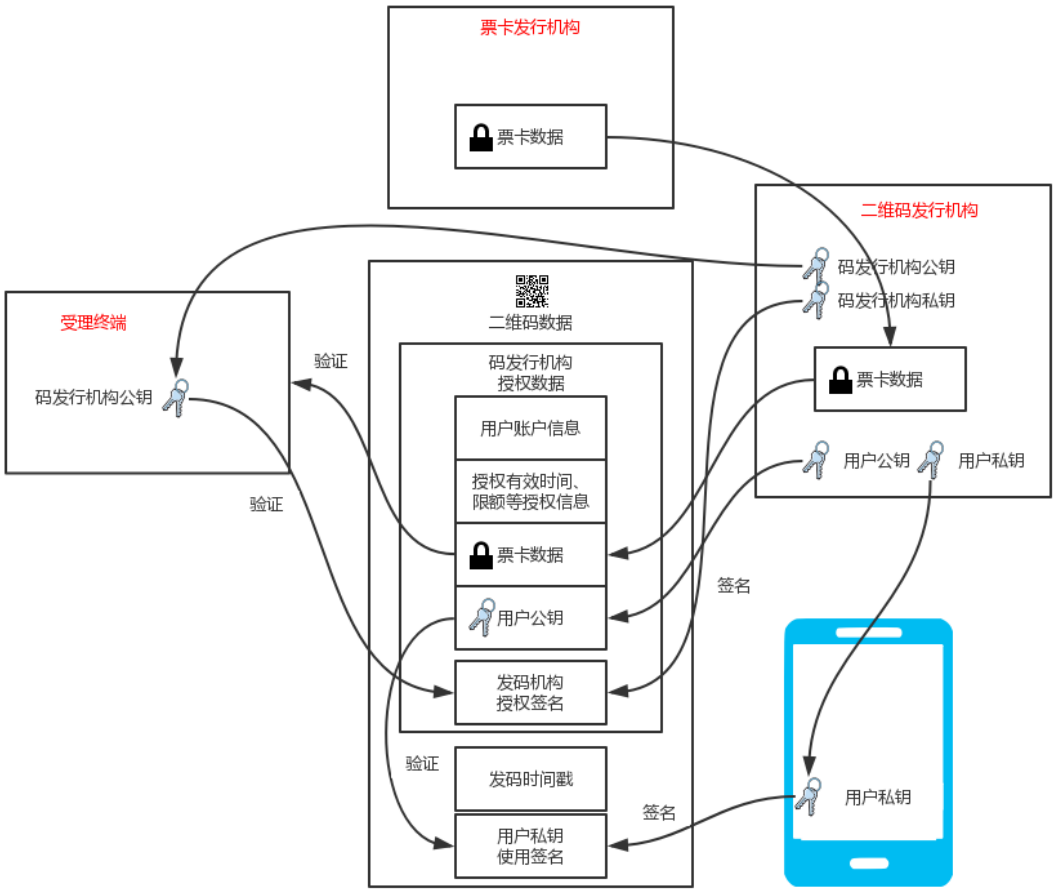

图 2 工作原理示意图

1) 票卡发行机构向用户发行二维码票卡，票卡发行机构可根据业务规则生成二维码票卡数据，对于票卡数据有机密性要求时，票卡发行机构可以对生成的票卡数据进行安全加密；
2) 票卡发行机构将二维码票卡数据发送给二维码发行机构，由二维码发行机构进行授权；
3) 二维码发行机构验证用户资质，使用机构私钥对二维码票卡数据进行签名授权；其中，签名是通过二维码发行机构的私钥产生，发码机构授权数据不可伪造且不可否认；
4) 用户使用二维码票卡时，使用用户私钥对时间戳和二维码发行机构的授权数据进行签名；时间戳控制生成的二维码有效时间范围，提高二维码复制泄露的难度和风险；签名通过用户私钥产生，用户使用数据不可伪造且不可否认；
5) 受理终端使用发码机构公钥验证发码机构签名合法性，再使用二维码中用户公钥验证用户签名合法性，根据发码时间戳验证二维码有效性；对有效的二维码提取原始票卡数据，根据受理终端与票卡发行机构约定的验证逻辑验证票卡数据有效性；票卡数据需要加密时，受理终端与票卡发行机构约定验证方法，包括加密算法、密钥规则等；
6) 受理终端受理票卡二维码后根据业务规则选择进行脱机交易或联机交易；

7） 支付机构受理请款请求，完成交易结算；

5.3. 工作流程【暂不对外提供】

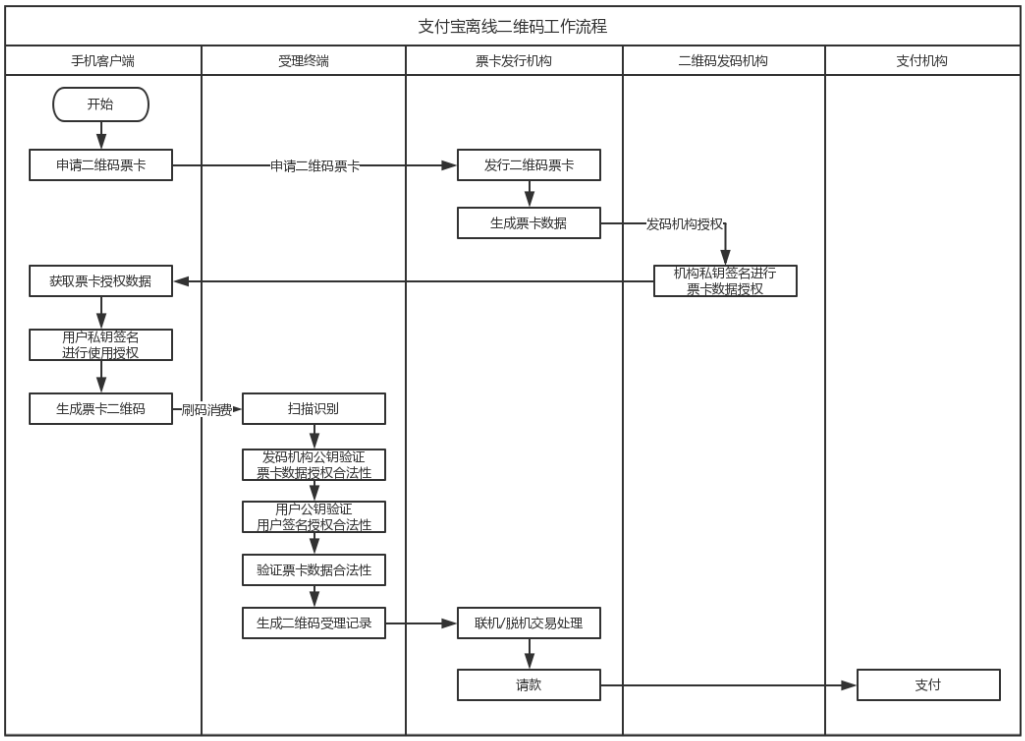

图 3 工作流程图

5.4. 应用模式

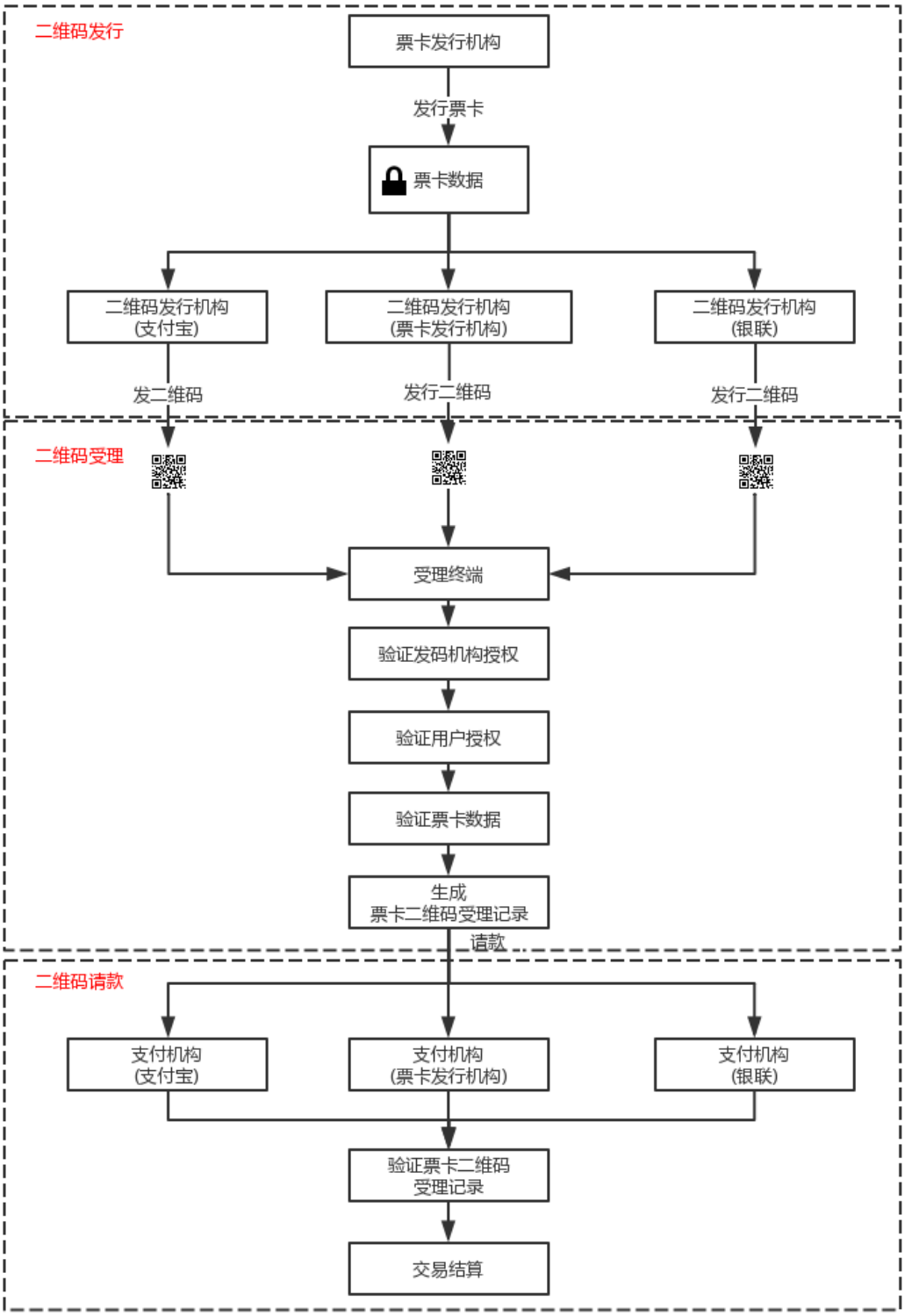
二维码发行
票卡发行机构
发行票卡
票卡数据
二维码发行机构
(支付宝)
二维码发行机构
(票卡发行机构)
二维码发行机构
(银联)
发二维码
发行二维码
发行二维码
二维码受理
受理终端
验证发码机构授权
验证用户授权
验证票卡数据
生成
票卡二维码受理记录
请款
二维码请款
支付机构
(支付宝)
支付机构
(票卡发行机构)
支付机构
(银联)
验证票卡二维码
受理记录
交易结算

图 4 应用模式

1) 票卡发行机构根据本规范生成票卡数据，票卡数据可选择多个二维码发行机构发行；
2) 受理终端使用二维码发行机构的公钥验证和受理票卡二维码，对通过验证的票卡二维码生成票卡二维码受理记录，进行联机或者脱机交易，向对应的支付机构进行请款；
3) 支付机构受理请款请求，验证票卡二维码受理记录，对有效请款请求进行交易结算处理；

5.5. 交易结算

二维码发行机构负责用户身份和二维码的安全性，支付机构负责用户交易和资金安全，二维码安全和资金安全有紧密关系，通常二维码发行与支付机构为同一主体；本规范不限制票卡发行机构、二维码发行机构和支付机构关系；有二维码发行能力的票卡发行机构可直接发行票卡二维码；有资金处理能力的票卡发行机构也可同时作为支付机构。

本规范支持票卡二维码进行联机交易和脱机交易。对于脱机交易场景，由于用户脱机交易时无法实时核验用户身份、信用和支付能力，可能发生用户使用票卡二维码进行脱机交易而实际交易结算时无法支付扣款。

二维码发行机构在发行二维码时应当严格验证用户身份信息，例如用户实名认证、信用记录、资产情况等，可选择接入支付宝、芝麻信用、银联等机构；当用户资质不满足或出现风险时立即停止为用户发行票卡二维码。

支付机构为用户脱机交易提供必要的信用担保，当用户无法支付时，支付机构提供担保资金确保完成脱机交易结算，同时可对用户进行必要的惩罚，例如停止提供服务，影响用户信息记录等。

5.5.1. 联机交易

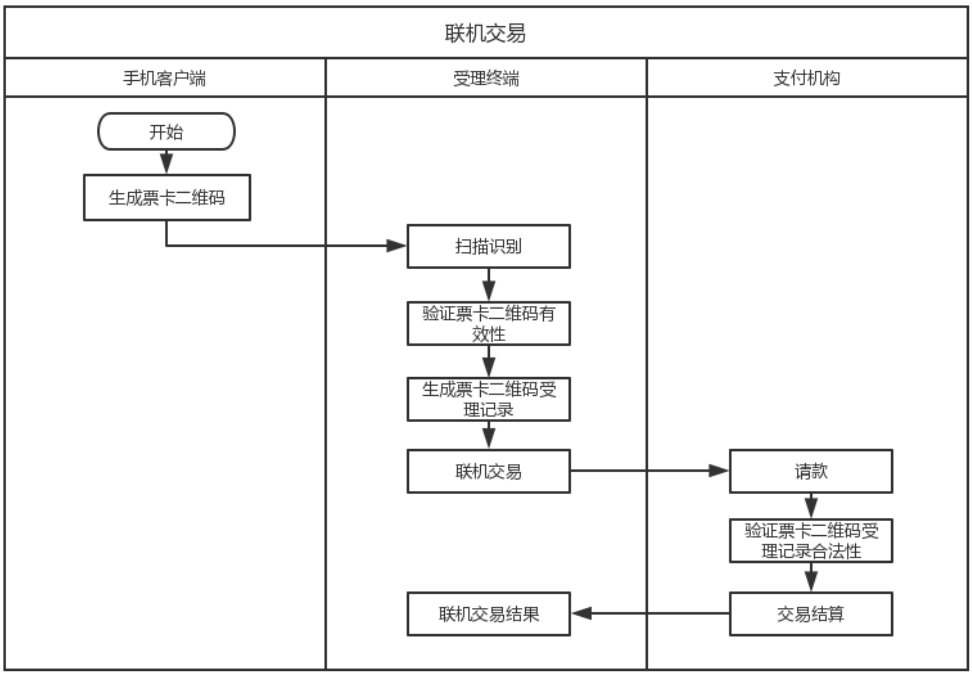

图 5 联机交易

用户使用票卡二维码进行联机交易，受理终端识别和验证票卡二维码，生成票卡二维码受理记录，向支付机构联机发起请款；支付机构验证票卡二维码受理记录合法性，完成交易结算后将支付结果同步返回受理终端。

二维码发行机构负责确保用户票卡二维码安全性，包括对用户身份的核验，二维码泄露风险控制等。

支付机构确保用户资金安全，根据实际风险条件判断如何进行支付，必要时可要求用户在线验证身份，如输入密码等，或者阻断联机交易。

5.5.2. 脱机交易

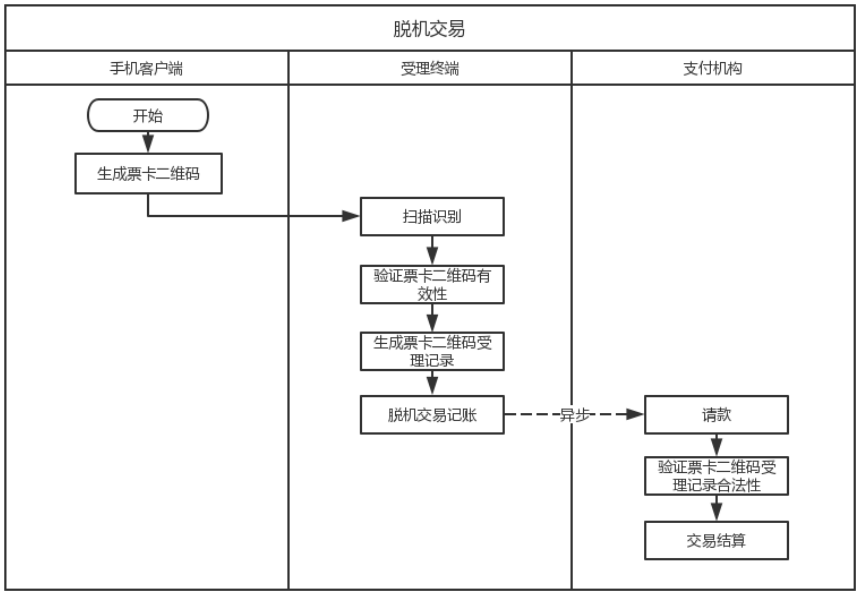

图 6 脱机交易

用户使用票卡二维码进行脱机交易，受理终端识别和验证票卡二维码，生成票卡二维码受理记录，本地进行脱机交易记账。事后异步向支付机构发起请款，支付机构验证票卡二维码受理记录合法性，完成交易结算。

二维码发行机构确保用户票卡二维码安全性，包括对用户身份的核验，二维码泄露风险控制等。

支付机构负责确保用户资金安全，对合法的脱机交易账单支付机构必须完成交易结算。

6. 二维码协议

6.1. 编码方式

采用二进制(8bit-byte）编码，模式标示符0100。

6.2. 纠错能力

不限制，建议L级(>=7%)。

6.3. 数据格式

二维码协议数据格式如图 7。

图 7 二维码协议格式

协议头												
二维码版本					算法版本				密钥ID			
1byte					1byte				1byte			
机构授权数据												
长度	uid	过期时间	码有效时间	限额	身份	机构编码	保留字段	用户公钥	票卡类型	票卡编码号	票卡数据	授权数据签名
1byte	16bytes	4bytes	2bytes	2bytes	4bytes	4bytes	4bytes	不定长	8bytes	不定长	不定长	不定长
用户授权数据												
长度		生码时间			用户签名							
1byte		4bytes			不定长							

6.3.1. 协议头部

字段	长度	说明	备注
二维码版本	1字节	定义二维码协议版本	
算法版本	1字节	定义二维码安全算法版本	支持版本： ➢ 1 机构授权签名算法 ECDSA256 用户授权签名算法 ECDSA192
密钥ID	1字节	定义二维码发行机构授权数据签名密钥编号	授权机构可通过密钥ID动态切换密钥

6.3.2. 机构授权数据

字段	长度	说明	备注

长度	1字节	机构授权数据长度	
用户ID	16字节	使用二维码的用户ID	
过期时间	4字节	机构授权数据有效时间，过期无效	使用UTC(0时区)时间1970年1月1日00:00:00到现在的秒数
二维码有效时长	2字节	二维码生成后的有效时长，过期无效	单位秒
限额	2字节	二维码允许的单笔交易限额	单位分
用户身份	4字节	表示特定用户的身份，例如学生身份	
机构编码	4字节	唯一确定二维码发行机构	二维码发行机构编码可向支付宝申请
保留字段	4字节	-	保留
用户公钥	不定	用户密钥对中的公钥	密钥长度和算法由协议头部算法版本确定
票卡类型	8字节	二维码代表的票卡类型	票卡发行机构与二维码发行机构约定
票卡编号长度	1字节	票卡编号的长度	
票卡编号	不定	票卡号码	
票卡数据长度	1字节	票卡数据长度	
票卡数据	不定	票卡数据	票卡发行机构自定义，数据可加密； 无票卡数据时为空；
授权数据签名长度	1字节	授权数据签名的长度	
授权数据签名	不定	二维码发行机构私钥对授权数据签名结果	签名算法由协议头部协议版本确定

6.3.3. 用户授权数据

字段	长度	说明	备注
长度	1字节	用户授权数据长度	
生码时间	4字节	二维码的生成时间	使用UTC(0时区)时间1970年1月1日00:00:00到现在的秒数
用户签名长度	1字节	用户签名的长度	
用户签名	不定长	用户私钥签名结果	

7. 受理记录协议

7.1. 编码方式

二进制编码。

7.2. 数据格式

头部信息	
受理记录协议版本	受理记录长度
4bit	12bit
二维码信息	
二维码长度	原始二维码
2bytes	不定长
受理终端信息	
受理终端信息长度	受理终端信息
2bytes	不定长
时间信息	
受理时间长度	受理时间
2bytes	不定长
完整性签名	
完整性签名长度	完整性签名
2bytes	不定长

7.2.1. 头部信息

字段	长度	说明	备注
受理记录协议版本	4比特	受理记录协议版本	
受理记录长度	12比特	受理记录长度	

7.2.2. 二维码信息

字段	长度	说明	备注
二维码长度	2字节	原始二维码信息长度	

二维码	不定长	原始二维码数据	二维码数据格式见二维码协议部分

7.2.3. 受理终端信息

字段	长度	说明	备注
受理终端ID	不定长	受理终端ID，唯一表示受理终端	
受理记录类型	不定长	区分联机、脱机等交易类型	
受理记录名称	不定长	描述本次票卡受理业务	
受理记录ID	不定长	受理记录唯一单据号	

7.2.4. 受理时间

字段	长度	说明	备注
受理时间长度	2字节	受理时间的长度	
受理时间	4字节	受理记录的时间戳	使用UTC(0时区)时间1970年1月1日00:00:00到现在的秒数

7.2.5. 完整性签名

字段	长度	说明	备注
完整性签名长度	2字节	完整性签名长度	
完整性签名	不定长	受理记录完整性签名	算法由受理终端与支付机构约定

8. 算法与密钥

8.1. 机构授权签名

8.1.1. 密钥

公私密钥对由二维码发行机构负责生成、存储和管理，建议使用KMI、加密机等密钥安全管理系统进行存储和访问。

私钥由二维码发行机构安全存储。

公钥公开同步到受理终端。

8.1.2. 算法

协议头部算法版本	算法	说明
1	ECDSA256	椭圆曲线secp256k1

8.2. 用户授权签名

8.2.1. 密钥

公私钥对由用二维码发行机构生成，由用户手机客户端进行安全存储，建议存储于TEE、黑匣子等手机安全存储区。

私钥由手机客户端进行安全存储。

公钥编码到二维码协议中。

8.2.2. 算法

协议头部算法版本	算法	说明
1	ECDSA192	椭圆曲线secp192k1

9. 安全规范

9.1. 存储安全

本规范涉及的关键数据需要进行安全保护，例如算法私钥等应当进行安全存储，防止信息泄露和篡改。

信息	二维码发行机构	手机客户端	受理终端
机构私钥	KMI 或加密机	不涉及	不涉及
机构公钥	可明文存储	不涉及	可明文存储
用户私钥	KMI 或加密机	手机安全存储区，例如 TEE，黑匣子	无
用户公钥	可明文存储	可明文存储	不保存
机构授权数据	不保存	手机安全存储区，例如 TEE，黑匣子	不保存
二维码受理记录	不涉及	不涉及	可明文存储，需防篡改

9.2. 传输安全

传输安全保护各主体之间进行信息传递的安全性，各主体间信息通信应当建立安全通信信道，例如https等。

9.3. 不可伪造和不可抵赖

数据	方法	说明
机构授权数据	机构私钥签名	不可仿造、不可抵赖
票卡二维码	用户私钥签名	不可仿造、不可抵赖
主体间请求应答报文	主体证书签名	不可伪造，不可抵赖

10. 手机客户端

10.1. CPU

具备一定的运算性能，支持100ms内根据本协议规范生成二维码。

10.2. 存储

具备安全存储能力，可安全存储用户私钥、机构授权数据等安全信息。

10.3. 显示

支持显示二维码，建议支持高亮、常亮、防截屏等功能。

10.4. 时钟模块

手机客户端应当定期进行时钟同步，确保与时钟服务器保持同步。

11. 受理终端

11.1. CPU

具备一定的运算性能，支持 200ms 内完成票卡二维码验证受理。

11.2. 存储器

安全、可靠存储二维码发行机构公钥。
安全、可靠存储票卡二维码受理记录。

11.3. 二维码读取器

可识别二进制编码格式二维码，支持识别旋转、倾斜、偏转二维码。

11.4. 显示屏

可选，建议支持票卡二维码受理信息显示。

11.5. 扬声器

可选，建议支持票卡二维码受理语音提示。

11.6. 时钟模块

定期进行时钟同步和矫正，与时钟服务器保持同步。

11.7. 通信模块

具备准实时数据传送和下载功能，支持联机/脱机交易请款报送，支持二维码发行机构公钥动态更新下载。