支付宝离线二维码开放协议

文档修改历史

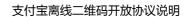
版本号	作者	内容提要	发布日期
V0.1	平楚	[C]文档初稿	20170627

*变化状态: C——创建, A——增加, M——修改, D——删除



目录

1	概这	<u>k</u>		5
2	术语	<u> </u>		5
3	协议	义		6
	3.1	支付:	宝乘车码	6
		3.1.1	协议结构	6
		3.1.2	字段说明	6
	3.2	二维	码电子卡	8
		3.2.1	协议结构	8
		3.2.2	字段说明	8
	3.3	脱机	记录	10
		3.3.1	协议结构	10
		3.3.2	字段说明	11
4	算法	Է		12
	4.1	算法	参数	12
		4.1.1	二维码算法	12
		4.1.2	脱机记录算法	13
	4.2	机构:	授权签名	13
		4.2.1	签名算法	13
		4.2.2	验证算法	13
	4.3	用户	授权签名	13





13	4.3.1	
14	4.3.2	
名 14	4 脱机i	4 4



1 概述

本文档描述支付宝离线二维码开放协议及相关算法的实现细节。

2 术语

名称	说明
支付宝乘车	支付宝乘车码特指支付宝发行的、在支付宝客户端提供的可在支持城市和
码	线路刷码乘车的二维码。
二维码电子	二维码电子卡是指由发卡公司发行的、在支付宝客户端提供的可在支持终
卡	端上刷码消费的二维码。
	脱机操作特是指用户使用离线二维码在商户终端进行刷码的行为。一次脱
	机操作会生成一条脱机记录,支付宝通过验证脱机记录的有效性识别脱机
脱机操作	 交易有效性。根据不同的场景,一笔脱机交易可能包括一笔或者多比脱机
	记录。例如,单程公交一笔交易包含一笔脱机操作,地铁交易则通常包括
	进展和出站两笔脱机记录。



3 协议

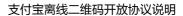
3.1 支付宝乘车码

3.1.1 协议结构

<u>tz</u>	心义	<u>-</u>		机构授权信息										
版	算	秘		机构授权数据										机构授权签名
本	法	钥	K	计 用户 ID 过期 码有效 单笔 身份					机构	保留	用户	签	签名	
		id	度	数		时间	时间	限额	信息	编号	字段	公钥	名	
				器									K	
													度	
1	1	1	1	1	16	4	2	2	4	4	4	不定	1	不定
							用户的	受权信息	<u>1</u>					
	用户授权数据								用户授	权签名				
长	长度 二维码生 签名长度						签名							
		瓦	战时间											
1	ļ		4	1					不定					

3.1.2 字段说明

字段	长度	说明	备注
版本	1byte	乘车码固定为 1	
算法	1byte	算法版本,当前 0	
密钥 ID	1byte	机构授权签名使用的主密	
		钥编号	
机构授权信息长度	1byte	表示机构授权数据长度	覆盖从计数器(包含)开始到
			用户公钥(包含)结束的数据





	l l		
			长度
计数器	1byte	机构授权数据计数器	
用户ID	16bytes	用户唯一 ID	
过期时间	4bytes	机构授权信息失效时间,	
		1970-01-01 00:00:00 开始	
		秒数	
二维码有效时间	2bytes	动态二维码有效时间 ,单位	
		秒	
单笔限额	2bytes	单笔消费额度上限 ,单位分	
身份信息	4bytes	用户身份类型,默认填充	
		{0x00 , 0x00 , 0x00 , 0x00}	
机构编号	4bytes	唯一表示发码机构	自主发码机构请向支付宝
		支付宝机构编号为:{0x00,	申请机构编号
		0x00 , 0x00 , 0x00}	
保留字段	4bytes	保留使用,目前填充{0x00,	
		0x00 , 0x00 , 0x00}	
用户公钥	不定长	用户公钥,长度由算法确定	
机构授权签名长度	1byte	表示机构授权签名字段长	
		度	
机构授权签名	不定长	根据签名算法计算的签名	签名计算方法参考算法说
		数据 ,长度由签名算法确定	明部分
用户授权数据长度	1byte	用户授权数据信息	覆盖二维码生成时间(包含)
			开始到二维码生成时间(包
			含)结束
二维码生成时间	4bytes	二维码生成时间,	
		1970-01-01 00:00:00 开始	
		秒数	
用户授权签名长度	1byte	表述用户授权签名字段长	



		度	
用户授权签名	不定长	用户授权签名,长度由算法	签名计算方法请参考算法
		确定	说明部分

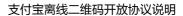
3.2 二维码电子卡

3.2.1 协议结构

<u>协议头</u>			机构授权信息								
二维码版	算法	秘钥		机			机构授	构授权数据			
本	版本	id	长度	用户 id	过期	码有	单笔	身份信	机构	保留	用户公钥
					时间	效时	限额	息	编号	字段	
						间					
1	1	1	1	16	4	2	2	4	4	4	不定
	机构授权信息										
	机构授权数据 机构授权签名										
卡类型	밑	卡号长	卡号	卡数据	卡数捷	居长	签名				
		度		长度							
8		1	不定	1	不定	. 1		不定			
					用戶	[〕] 授权信	息				
用户	授权数据	3					用户授	权签名			
长度 二维码生			K	度			签名				
	成	时间									
1 4					1					不定	

3.2.2 字段说明

字段	长度	说明	备注





			Τ'
版本 1	lbyte	二维码电子卡版本为 2	
算法 1	lbyte	算法版本,当前 0	
密钥 ID 11	lbyte	机构授权签名使用的主密	
		钥编号	
机构授权信息长度 1	lbyte	表示机构授权数据长度	覆盖从用户 ID (包含)开始
			到卡数据(包含)结束的数据
			长度
用户 ID 16	16bytes	用户唯一 ID	
过期时间 4	4bytes	机构授权信息失效时间,	
		1970-01-01 00:00:00 开始	
		秒数	
二维码有效时间 2	2bytes	动态二维码有效时间,单位	
		秒	
单笔限额 2	2bytes	单笔消费额度上限 ,单位分	
身份信息 4	4bytes	用户身份类型,默认填充	
		{0x00 , 0x00 , 0x00 , 0x00}	
机构编号 4	4bytes	唯一表示发码机构	自主发码机构请向支付宝
		支付宝机构编号为:{0x00,	申请机构编 号
		0x00 , 0x00 , 0x00}	
保留字段 4	4bytes	保留使用,目前填充{0x00,	
		0x00 , 0x00 , 0x00}	
用户公钥	不定长	用户公钥 ,长度由算法确定	
卡类型 8	Bbytes	二维码电子卡类型 , 唯一表	新增卡类型请向支付宝申
		示一种卡类型	请分配
卡号长度 1	lbyte	表示卡号长度	
卡号 7	不定长(不超过 16bytes)	唯一表示一张卡,由卡号长	卡号由发卡机构自主分配
		度确定	
卡数据长度 1	lbyte	表示卡数据长度	



卡数据	不定长(不超过 64bytes)	电子卡数据 , 由卡数据长度	卡数据由发卡机构自主设
		确定	置
机构授权签名长度	1byte	表示机构授权签名字段长	
		度	
机构授权签名	不定长	根据签名算法计算的签名	签名计算方法参考算法说
		数据 ,长度由签名算法确定	明部分
用户授权数据长度	1byte	用户授权数据信息	覆盖二维码生成时间(包含)
			开始到二维码生成时间(包
			含)结束
二维码生成时间	4bytes	二维码生成时间,	
		1970-01-01 00:00:00 开始	
		秒数	
用户授权签名长度	1byte	表述用户授权签名字段长	
		度	
用户授权签名	不定长	用户授权签名,长度由算法	签名计算方法请参考算法
		确定	说明部分

3.3 脱机记录

3.3.1 协议结构

<u>头部信息</u>		
记录版本	记录长度	
4bit	12bit	
原始二维码长度	原始二维码数据	



2bytes	不定长		
终端信息			
终端信息长度	终端信息数据		
2bytes	不定长		
受理时间			
终端时间长度	终端时间		
2bytes	不定长		
<u>软件版本</u>			
软件版本长度	软件版本		
2bytes	不定长		
完整性签名			
签名长度	完整性签名		
2bytes	不定长		

3.3.2 字段说明

字段	长度	说明	备注
记录版本	4bits	版本为 2	
记录长度	12bites	记录数据长度 ,从原始二维	
		码长度(包含)开始到结尾的	
		数据长度	
原始二维码长度	2bytes	表示原始二维码数据长度	
原始二维码数据	不定长	原始二维码数据内容,长度	



		由原始二维码长度确定	
终端信息长度	2bytes	表示终端信息长度	
终端信息	不定长	终端信息内容	json 格式终端信息
终端时间长度	2bytes	表示受理时间	
终端时间	不定长	受理时间, 1970-01-01	
		00:00:00 开始的秒数	
软件版本长度	2bytes	表示软件版本数据长度	
软件版本	不定长	建议版本分配方式: 例:0000.0.2.0.20170	
		机具商户号.大版本.子版本.	
		紧急版本.迭代版本	
完整性签名长度	2bytes	表示完整性签名数据长度	
完整性签名	不定长	完整性签名	密钥使用用户 ID

4 算法

4.1 算法参数

4.1.1 二维码算法

算法版本	机构授权签名	用户授权签名	备注
0x00	算法: ecdsa256	算法: ecdsa192	ecdsa 算法请参考标
	曲线: secp256k1	曲线: secp192k1	准 X9.62
	公钥: 点压缩	公钥: 点压缩	实现可参考 openssl



4.1.2 脱机记录算法

版本	完整性签名	备注
0x02	算法: hmac-md5	hmac-md5 算法请参考
		RFC2104
		实现可参考 openssl

4.2 机构授权签名

4.2.1 签名算法

使用【算法版本指定的机构授权签名算法】和【机构编号和主密钥 ID 指定的机构私钥】对 【机构授权信息长度字段指定的数据】执行数据签名。

4.2.2 验证算法

使用【算法版本指定的机构授权签名算法】和【机构编号和主密钥 ID 指定的机构公钥】对 【机构授权信息长度字段指定的数据】执行数据验签。

4.3 用户授权签名

4.3.1 签名算法

使用【算法版本指定的用户授权签名算法】和【用户公钥对应的用户私钥】对【从头部信息开始(包含)到用户授权数据长度(不包括)为止的数据】执行数据签名。



4.3.2 验签算法

使用【算法版本指定的用户授权签名算法】和【用户公钥】对【从头部信息开始(包含)到用户授权数据长度(不包括)为止的数据】执行数据验签。

4.4 脱机记录完整性签名

以用户 id 作为密钥,使用 hmac-md5 对【受理记录版本(包含)到完整性签名长度(不包含)的数据】执行完整性签名。