前言

第1章 文档概述

1.1 介绍

1.1.1 概述

1.1.2 目标读者

本文的主要目标读者是商户的技术实施人员。

1.1.3 版本规范

1.1.4 最近修订

版本号	作者	内容提要	核准人	发布日期
1.0	王苗淼	初始创建	杨涛	2011-5-31
1.0	金其林	精简错误代码说明	杨涛	2011-7-19
1.1	陈宝航	增加单笔退货接口	杨涛	2011-11-18
1.3	贾云	增加退货结果文件金额格式	范春	2014-11-04

1.2 参考标准与文献

第2章 系统架构

2.1 交互模式

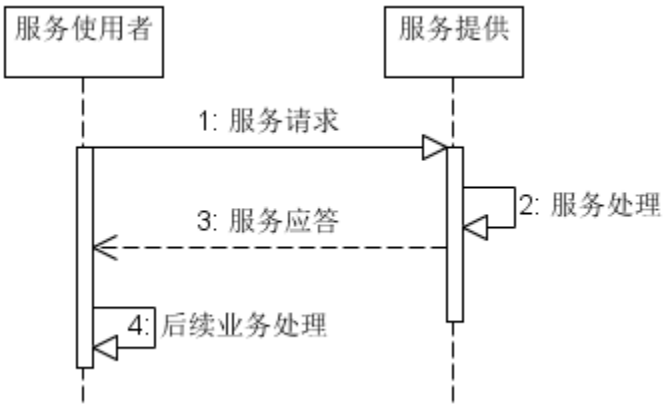
在网上支付退货业务的技术实现中，商户与银行之间通过交换报文来交换业务信息、实现业务流程、控制业务规则。

实现网上支付退货业务所需的交互模式为请求-应答模式。

2.1.1 请求-应答模式

在请求-应答模式下，一方作为服务提供者，另一方作为服务使用者。由服务使用者主动向服务提供者发起请求并等待应答，服务提供者接受请求，完成处理，并向服务使用者应答处理结果，服务使用者收到处理结果之后进行后续处理。

请求-应答模式适用于服务使用者需要根据服务提供者的服务应答才能进行正确的后续处理的场景，比如，在网上支付业务中，商户作为服务使用者，银行作为服务提供者，商户需要知道银行的支付处理结果之后才能继续交易流程。



第3章　业务实现规范

网上支付退货业务功能包含退货、批量退货等功能，其中退货功能，商户需要按照技术规范进行开发接入，批量退货功能则基于企业网银现有功能实现，商户无需开发即可在企业网银中实现退货功能。

本章描述商户与银行之间的业务流程与规则。同时，本章也规定了在商户与银行快捷支付业务间的交互模式、交换的报文规范。

3.1 接口实现说明

序号	接口类型	实现方式
1	单笔退货	商户接入（选做）
2	批量退货	企业网银（已实现）

3.2 单笔退货

3.2.1 业务功能

本交易提供给商户进行快捷支付单笔实时退货。

3.2.2 业务规则

单笔退货业务在执行中需要满足以下约束条件：

- 银行根据商户请求信息实时返回退货结果，返回正常退货结果代表退货成功，返回错误的代表退货失败。
- 同一退货订单号的退货交易银行保证只执行一次。
- 单笔退货支持全部金额退货、部分金额退货、以及对同一笔支付订单进行多次退货。
- 单笔退货采用单独的接入地址，请参见单笔退货接入地址。

3.2.3 处理流程

由商户发起单笔退货请求指令至银行，银行端根据请求指令中的退货订单信息进行退货，并将退货结果返回给商户。

3.2.4 交互模式

在单笔退货业务中，商户与银行通过请求-应答模式交互。
商户作为服务使用者向银行发送“单笔退货”请求报文 **CSRReq**，银行作为服务提供者向商户返回“单笔退货”应答报文 **CSRRes**。

3.2.5 报文格式

- **“单笔退货”请求报文 CSRReq(Common Single Refund Request)**

单笔退货请求报文是从商户向银行发起的提现请求。

中文域名	对应元素	类型	是否必输	说明
交易代码	transId	char(10)	是	**CSRReq**
商户号	merId	char(12)	是	商户在银行开通的商户代码
商户流水号	serialNo	char(19)	是	对应商户的退货订单号
商户日期和时间	date	char(17)	是	YYYYMMDD HH:MM:SS
原商户流水号	originalSerialNo	char(19)	是	对应商户的原支付订单号
原商户日期和时间	originalDate	char(17)	是	YYYYMMDD HH:MM:SS
交易金额	amount	long(12)	是	以元为单位，详情见金额格式说明

- **“单笔退货”应答报文 CSRRes(Common Single Refund Response)**

单笔退货应答报文是银行返回给商户的应答。

中文域名	对应元素	类型	是否必输	说明
交易代码	transId	char(10)	是	**CSRRes**
商户号	merId	char(12)	是	商户在银行开通的商户代码

商户流水号	serialNo	char(19)	是	对应商户的退货订单号
商户日期和时间	date	char(17)	是	YYYYMMDD HH:MM:SS
清算日期	clearDate	date(8)	是	YYYYMMDD

3.3 批量退货

3.3.1 业务功能

批量退货的业务目的是在发生支付之后，将该笔交易支付的款项原路退回到客户银行卡账户中。

批量退货以提供批量退货指令文件的方式，商户需要按约定格式组织批量退货请求文件，登陆企业网银进行批量退货文件的上传、退货结果的查询及结果文件的下载。

3.3.2 业务规则

批量退货业务在执行中需要满足以下约束条件：

- 商户应严格按照文件格式及最大笔数限制生成文本文件并上传。
- 商户需要在企业网银中上传请求文件，并查询退货结果及下载结果文件。
- 商户如果退货交易量非常少，则应优先选择企业网银中的直接退货功能进行单笔退货。
- 商户应保证批量退货请求文件中的每一笔退货明细对应的原支付交易状态为明确成功。
- 批量退货支持全部金额退货、部分金额退货、以及对同一笔支付订单进行多次退货。

3.3.3 处理流程

在“批量退货”业务中，商户需要登陆企业网银进行批量退货请求文件的上传及批量退货结果文件的下载。

3.3.4 交互模式

在“批量退货”业务中，商户需要登陆企业网银进行批量退货请求文件的上传及批量退货结果文件的下载。

3.3.5 文件格式

上传文件格式要求：

总金额

总笔数

流水号（订单号）、交易日期、预留字段、退货金额、交易货币代码、原流水号、原交易日

期、摘要

说明：

- 文件类型：文本文件（*.txt）。
- 退货最大笔数：2000 笔。
- 分隔符：“,”为英文模式下的逗号。
- 文件头：
  总金额：**以元为单位**，例如：1234.35 （为英文模式下的数字）
  总笔数：整数
- 字段要求，如下表：

字段名称	**格式**	**要求**
商户退货流水	VARCHAR(30)	非空，同一日期不能重复，建议最少长度为 6 位
商户退货日期	YYYYMMDD 00:00:00	非空，由商户定义
预留字段	VARCHAR(45)	暂时送空
金额	100.96(元)	非空，退货金额
币种	人民币	非空，固定送 156
原交易订单	VARCHAR(30)	非空,该笔退货原交易的订单号
原交易日期	YYYYMMDD	非空,该笔原交易发生的日期
摘要	VARCHAR(30)	非空，商户自己定义

- 文件内容示例：

16.56
2
956975212,20081030 17:00:09,,5.00,156,500070213,20081030,退货
958794212,20081031 11:00:04,,11.56,156,511896721,20081022,退货

- 文件结尾不能有回车换行,每笔退货记录为一个完整行，不能分行。

结果文件格式要求：

处理成功总金额

处理成功总笔数

处理失败总笔数

流水号（订单号）,交易日期,预留字段,退货金额,交易货币代码,原流水号,原交易日期,处理状态,失败原因,摘要

说明：

- 返回文件为文件文件（*.txt）。
- 处理成功总金额：1234.56（为英文模式下的数字）。
- 处理成功总笔数：整数。
- 处理失败总笔数：整数。
- 字段要求，如下表：

字段名称	格式	要求
商户退货流水	VARCHAR(30)	商户提交的退货流水
商户退货日期	YYYYMMDD 00:00:00	商户提交的退货日期
协议号	VARCHAR(45)	暂时送空
金额	100.96(元)	商户发起退货金额
币种	人民币	固定送 156
原交易订单	VARCHAR(30)	该笔退货原交易的订单号
原交易日期	YYYYMMDD	该笔原交易发生的日期
处理状态	Y/N	Y 成功，N 失败
结果	VARCHAR(30)	如果处理状态为 Y，显示为退货成功 如果处理状态 N，为失败的具体原因
摘要	VARCHAR(30)	商户提交退货文件的摘要

■ 结果文件内容示例：

400.35
2
0
9770743232,20081106 16:22:19,,300.23,156,10339554,20081104,Y,交易成功,退货
9783023232,20081106 22:25:42,,100.12,156,20395992,20081106,Y,交易成功,退货

注：金额格式——1 元就显示 1，不会显示 1.0 或 1.00。

第4章 报文规范

报文规范是网上支付退货技术标准中重要的组成部分，规定了商户与银行之间交换报文的顺序、格式、语义与处理规范。本章中介绍报文的一般结构与公共元素，这些规范适用于单笔退货报文。

4.1 报文结构

网上支付单笔退货报文统一采用 xml 格式（见附录）。报文以 MessageSuit 作为根元素，每个 MessageSuit 元素中可以包含多个 Message 元素。Message 元素中包含代表具体数据的元素，比如 Plain、Signature 等。每个数据元素由一系列属性元素构成。

作为约定，MessageSuit 元素、Message 元素与业务元素均是首字母大写的 CamelCase 形式，所有的属性元素均是首字母小写的 CamelCase 形式。

以客户验证请求报文为例，报文的格式如下：

```
< MessageSuit>
  <Message id="901239052203">
    <Plain id=" USCReq">
        <version>1.0.1</ version>
        <transId>USCReq</transId>
```

```
            <merId>370310000004</merId>
            <relatedAcct>MerchantAccount</relatedAcct>
            <date>20110531120000</date>
            <name>陈广荣</name>
            <cardNo>6226690200028929</cardNo>
            <cardType>D</cardType>
            <validDate></validDate>
            <cvv2></cvv2>
            <certType>320326197712010642</certType>
            <certNo>1</certNo>
            <phone>13000000000</phone>
            <bussType>1</bussType>
        </ Plain>
        <Signature>…</Signature>
    </Message>
</ MessageSuit>
```

4.2 报文分类

报文按照交互模式的不同，分为以下几类：

■ 服务请求类报文

服务请求类报文用于请求-应答交互模式，由服务使用者向服务提供者发送。服务请求类报文的命令规范是 XXReq，其中 XX 是报文代表的业务的首字母缩略，Req 是 Request 的缩写。比如对于单笔退货请求报文，命名为 **CSRReq**，代表 **C**ommon **S**ingle **R**efund **R**equest。

■ 服务应答类报文

服务应答类报文用于请求-应答交互模式，由服务提供者向服务使用者返回。服务应答类报文的命令规范是 XXRes，其中 XX 是报文代表的业务的首字母缩略，Res 是 Response 的缩写。比如对于单笔退货应答报文，命名为 **CSRRes**，代表 **C**ommon **S**ingle **R**efund **R**esponse。

■ 通用报文

通用报文适用于所有的协议业务。网上支付单笔退货中的通用报文为 Error 报文，用于当请求不能被正确处理时的应答返回。

对于和业务相关的服务请求类、服务应答类报文的具体格式，将放在具体的业务实现规范中加以描述。通用报文将在本章描述。

4.3 通用报文

4.3.1 错误消息报文 Error

■ **功能**

用来当请求不能被正确处理时应答返回

■ **Error 域**

下表列举了 Error 消息域的定义

中文域名	字段名	类型	是否必输	说明
交易代码	transId	char (10)	是	Error
商户号	merId	char (12)	是	
错误代码	errorCode	char(4)	是	
错误描述	errorMessage	char(256)	是	
详细错误信息	errorDetail	char(512)	是	

■ **错误代码说明**

下表列举了标准的错误代码：

错误代码	**错误描述**	**解释**
程序类错误		
0002	必填域缺失	接口中必输项没有送值
0125	账户类型错误	银行卡的类型不支持此项业务
0212	商户校验失败	该商户不支持网上支付业务/该商户的服务类型不是快捷支付
0400	支付流水重复	重复的网上支付流水
用户类错误（可以将错误信息显示给用户）		
1605	银行交易失败	该笔交易在银行系统中已经失败，且状态不会再发生变更。错误具体详情通过 ErrorDetail 告知
管理类错误		
2000	支付渠道关闭	没有开通网上支付业务
系统类错误		
9000	暂时系统异常	例如，系统参数正在处理中。

4.4 报文的解析与传输

网上支付单笔退货报文的传输使用 XML Over HTTPS 方式，在 HTTP 请求/响应体中包含 XML 形式的报文。

4.4.1 报文解析

对 XML 解析的基本要求如下：

- **xml 解析**

为了可以支持后续协议版本，xml 解析的实现不要做严格的验证。特别是需要忽略未被确认的域。所有 xml 消息必须用“UTF-8”编码。

- **Message 域之 id 属性匹配**

请求和应答报文的 **Message** 域之 id 属性必须相同，id 是请求方生成的唯一序列号。比如：商户在 USCReq 的 Message 域设置了一个 id 属性值，则银行在 USCRes 里面的 Message 域的 id 属性则与 USCReq 的 Message 域之 id 值相同。

4.4.2 报文传输

对 HTTPS 传输的基本要求如下：

- **使用 POST 发送消息**

消息请求基于 HTTPS 的 POST 方式。

- **HTTP 消息头要求**

HTTP请求与响应消息中必须按照如下要求设置头部域：
‘**Content-Length:**’必须设置成消息体的长度
‘**Content-Type:**’必须设置下面的值：**application/xml; charset=utf-8**

第5章　信息安全规范

本章主要从技术角度阐述协议系统中可能出现的安全威胁，以及通过技术规范来规避安全风险的方式。

5.1 安全威胁

快捷支付业务涉及到商户与银行系统通过公众互联网络交换信息与指令。因此，在快捷支付信息安全规范中，我们主要对来自网络的安全威胁进行分析。对于来自内部系统与人员的安全风险，由银行与商户现有的安全体系来保障。

来自网络的安全威胁主要有以下几种：

- 交易指令篡改

如果网络中传输的协议交易指令被入侵者截获并篡改，就会造成资金处理出现错误，给快捷支付业务参与方造成损失。因此，在网络传输中，需要保证指令完整性。

解决方案：使用数字证书对对报文中的业务数据进行签名（见数字签名）。

■ 交易指令伪造

如果有入侵者冒充商户或者银行发起交易指令，就会造成资金在未得到快捷支付业务参与方的授权下发生流动，给银行、商户或客户带来损失。因此，在网络传输与系统处理中，需要保证指令的真实性。

解决方案：使用数字证书对对报文中的业务数据进行签名（见数字签名）。

■ 交易指令否认

当发生交易纠纷时，双方需要通过交易指令确定责任方。快捷支付安全规范中需要为交易指令防否认提供技术支持。

解决方案：使用数字证书对对报文中的业务数据进行签名（见数字签名），银行与商户均应保留涉及资金变动的交易报文日志（见报文日志管理）。

■ 交易指令重播

入侵者也可能尝试通过截获网络中传输的快捷支付交易指令，并多次重播的方式试图发起未经授权的交易。在快捷支付技术规范中，需要防止交易指令重播引起的未授权交易。

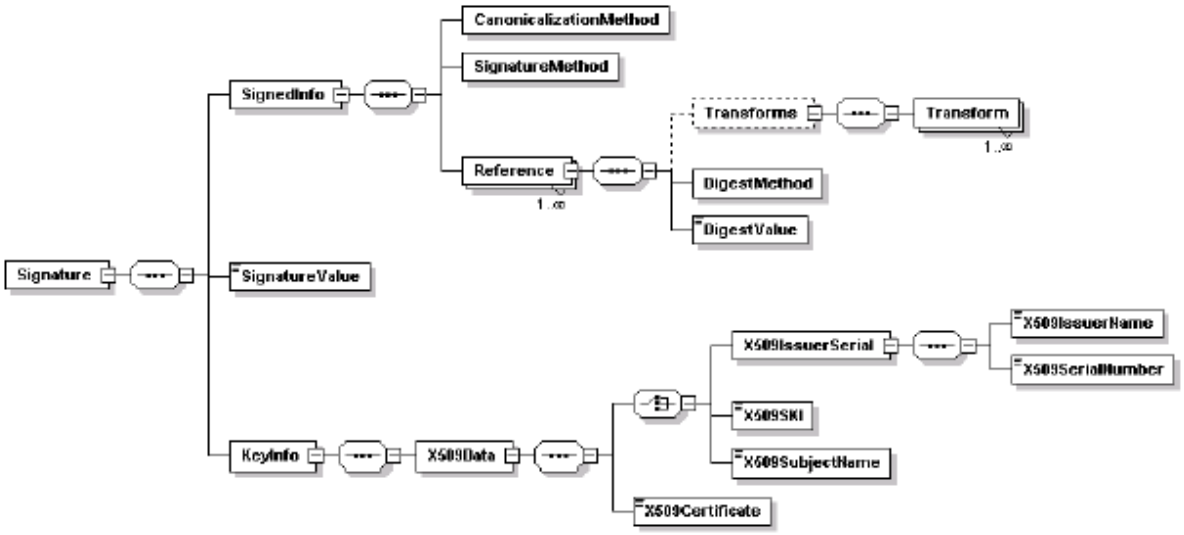
解决方案：凡涉及到资金变动的交易指令，流水号必须唯一。银行与商户均需要保证同一流水号的交易指令只能执行一次。

5.2 数字签名

5.2.1 数字签名要求

必须采用本节所述方法对 MessageSuit 消息进行数字签名。签名规范遵循 XML-Signature Syntax and Processing, W3C Recommendation 规范（http://www.w3.org/TR/xmldsig-core/）。

MessageSuit 协议使用分离签名（Detached signature），即<Signature> 元素与被签名的元素各自独立存在。被签名的元素和 <Signature> 元素包含在同一文档中。签名元素通过当地引用（如’# Plain1234’）被引用。被签名的元素内容包括从 Plain 等开始标签的开始括号开始到 Plain 等结束标签的结束括号为止的内容。



签名结构图

MessageSuit 签名的产生必须满足下列表格中定义的元素内容和算法要求。

表1 XML Signature Profile

元素	要求
Signature	没有KeyInfo实例；没有Object实例
CanonicalizationMethod	元素为空，但出现Algorithm属性
SignatureMethod	元素为空，但出现Algorithm属性
Transforms	存在且都包含一个Transform的实例
Transform	元素为空，但出现Algorithm属性
DigestMethod	元素为空，但出现Algorithm属性
KeyInfo	不出现。

表2 XML 签名算法

算法类型	标识符
Canonicalization	http://www.w3.org/TR/2001/REC-xml-c14n-20010315
Digest	http://www.w3.org/2000/09/xmldsig#sha1
Encoding	http://www.w3.org/2000/09/xmldsig#base64
Signature	http://www.w3.org/2000/09/xmldsig#rsa-sha1
Transform	http://www.w3.org/2000/09/xmldsig#enveloped-signature

5.2.2 规范化要求

注意：规范化是 “XML-Signature Syntax and Processing, W3C Recommendation”中的要求之一，也叫作xmldsig。

Xmldsig 表示计算同样文档的摘要必须使用规范化的方法。

5.2.3 签名的 XML 命名空间

消息的签名必须被声明在一个缺省的命名空间：http://www.w3.org/2000/09/xmldsig#中。

示例：

```
< MessageSuit>
    <Message id="901239052203">
        <Plain id="USCReq">
            <version>1.0.1</ version>
            <transId>USCReq</transId>
            <merId>370310000004</merId>
            <relatedAcct>MerchantAccount</relatedAcct>
            <date>20110531120000</date>
            <name>陈广荣</name>
            <cardNo>6226690200028929</cardNo>
            <cardType>D</cardType>
            <validDate></validDate>
            <cvv2></cvv2>
            <certType>320326197712010642</certType>
            <certNo>1</certNo>
            <phone>13000000000</phone>
            <bussType>1</bussType>
        </ Plain>
        <Signature xmlns="http://www.w3.org/2000/09/xmldsig#">
            <SignedInfo>
                <CanonicalizationMethod
                    Algorithm="http://www.w3.org/TR/2001/REC-xml-c14n-20010315">
                    </CanonicalizationMethod>
                <SignatureMethod
                    Algorithm="http://www.w3.org/2000/09/xmldsig#rsa-sha1">
                    </SignatureMethod>
                <Reference URI="#TSReq">
                    <Transforms>
                        <Transform
                            Algorithm="http://www.w3.org/2000/09/xmldsig#enveloped-signature">
                            </Transform>
                    </Transforms>
                    <DigestMethod
                        Algorithm="http://www.w3.org/2000/09/xmldsig#sha1">
                        </DigestMethod>
                    <DigestValue>4t79dXZ7/BQqgiBdkziaKTUslVU=</DigestValue>
                </Reference>
            </SignedInfo>
```

```
                <SignatureValue>

    RyWMXvxlhmLuOIOvGSIkpV1iRV400F1B2W0zmW9nc5qfvfNMtpyp+uNwksBUjcO8H//NW4GvxcDd
                KMuuc6k5MDMH1E4OUg+624FUY23qs3R2ztubtD3MU7xk4f0iq9L16GK4ZBeID/Lyj6CxjaCcp3Fu
                K1CznNj4Kr+qRLtxx+s= </SignatureValue>
            </Signature>
        </Message>
</ MessageSuit >
```

5.3 报文日志管理

为了做到交易指令防否认，银行与商户均应保留涉及资金变动的交易报文日志，日志中包括完整的报文、报文签名、接收时间，保存时间不小于 90 天。

交易报文日志应该妥善管理，避免泄密或者被破坏。

第6章 其它规范

6.1 异常处理规范

凡是报文验证不通过，或者业务处理失败，统一返回通用错误报文 Error。通用错误报文 Error 的格式参见 5.3.1 节。

6.2 错误码规范

错误码包含两部分，一部分是标准错误码，由快捷支付标准规定，参见 5.3.1 节。另一部分是商户特定代码，由商户自行规定。

第7章 附录

7.1 报文格式 DTD

```
<?xml version="1.0" encoding="UTF-8"?>
<!ELEMENT MessageSuit(Message)+>
<!ELEMENT Message (Plain, Signature) >
<!ATTLIST Message id ID #REQUIRED>

<!ELEMENT Plain (version,transId,merId,relatedAcct?,date?,name?,cardNo?,cardType?,validDate?,cvv2?,certType?,certNo?,phone?,bussType?,stageFlag?,stages?,serialNo?,charge?,amount?,currency?,goods?,subMerName?,clearDate?,type?,originalSerialNo?,originalDate?,status?,errorCode?,errorMessage?,errorDetail?,Signature)>
```

```
<!ATTLIST Plain id NMTOKEN #REQUIRED>
<!-- 属性 -->
<!ELEMENT version (#PCDATA)>
<!ELEMENT transId (#PCDATA)>
<!ELEMENT merId (#PCDATA)>
<!ELEMENT relatedAcct (#PCDATA)>
<!ELEMENT date (#PCDATA)>
<!ELEMENT name (#PCDATA)>
<!ELEMENT cardNo (#PCDATA)>
<!ELEMENT cardType (#PCDATA)>
<!ELEMENT validDate (#PCDATA)>
<!ELEMENT cvv2 (#PCDATA)>
<!ELEMENT certType (#PCDATA)>
<!ELEMENT certNo (#PCDATA)>
<!ELEMENT phone (#PCDATA)>
<!ELEMENT bussType (#PCDATA)>
<!ELEMENT stageFlag (#PCDATA)>
<!ELEMENT stages (#PCDATA)>
<!ELEMENT serialNo (#PCDATA)>
<!ELEMENT charge (#PCDATA)>
<!ELEMENT amount (#PCDATA)>
<!ELEMENT currency (#PCDATA)>
<!ELEMENT goods (#PCDATA)>
<!ELEMENT subMerName (#PCDATA)>
<!ELEMENT clearDate (#PCDATA)>
<!ELEMENT type (#PCDATA)>
<!ELEMENT originalSerialNo (#PCDATA)>
<!ELEMENT originalDate (#PCDATA)>
<!ELEMENT status (#PCDATA)>
<!ELEMENT errorCode (#PCDATA)>
<!ELEMENT errorMessage (#PCDATA)>
<!ELEMENT errorDetail (#PCDATA)>
<!ELEMENT Signature (#PCDATA)>
```

7.2 金额格式

金额以元为单位，保留小数点后 2 位，最多 12 位。例如：如果交易金额为 123.45，即表示一百二十三元四角五分。

7.3 货币代码表

快捷支付报文中的货币代码（currency 元素）的取值遵照国家标准 GB/T 12406-1996《表示货币和资金的代码》，该标准中规定了代表货币和资金的三个字母代码和与之等价的三位

数字代码的结构，说明了货币单位与货币之间十进制的关系，确立了维护代理机构的建立过程，并详细说明了代码应用方法。

根据 GB/T 12406-1996，货币代码字段使用 3 位定长数字，如下表所示：

国家、地区名称	货币名称	货币代码
中国	人民币元	156
中国香港	港元	344
中国澳门	澳门元	446
美国	美元	840
英国	英镑	826
法国	法国法郎	250
德国	马克	278
俄罗斯	卢布	810
日本	日元	392
加拿大	加元	124
瑞士	瑞士法郎	756
瑞典	瑞典克朗	752
意大利	意大利里拉	380
西班牙	西班牙比塞塔	724
葡萄牙	葡萄牙埃斯库多	620
荷兰	荷兰盾	528
比利时	比利时法郎	056
芬兰	马克	246
挪威	挪威克朗	578
希腊	德拉克马	300
奥地利	先令	040
丹麦	丹麦克朗	208
澳大利亚	澳大利亚元	036
新西兰	新西兰元	554
巴西	克鲁赛罗	076
南非	兰特	710
埃及	埃及镑	818
伊拉克	伊拉克第纳尔	368
伊朗	伊朗里亚尔	364
沙特阿拉伯	沙特里亚尔	682
科威特	科威特第纳尔	414
阿联酋	UAE 迪拉姆	784
泰国	铢	764
新加坡	新加坡元	702
印尼	卢比	360
马来西亚	马来西亚林吉特	458
菲律宾	菲律宾比索	608
南朝鲜	圆	410

印度	印度卢比	356

7.4 接入地址

测试环境单笔退货接入地址：https://219.143.234.251/agreeEpayper/payAccess.do
生产环境单笔退货接入地址：https://www.cebbank.com/agreeEpay/payAccess.do