2010

Alipay General Payments API Specification

In 2004, Alibaba Corporation established
its subsidiary-Alipay.com.
Alipay is committed to providing payment services with
"simple, secure and speedy" solutions to Chinese e-business.

Contents

1. Introduction

1.1. Overview

The Alipay General Payments API Specification is a description of the interface between the Client-side System and the Alipay Payments platform. .

The specification sets the unified standard for modes of interactions, data exchange and security between the Client-side System and the Alipay Payments System. General business support for payments and workflow process is also described in this documentation.

Intended Audience : Merchant Developers

2. Interaction Modes
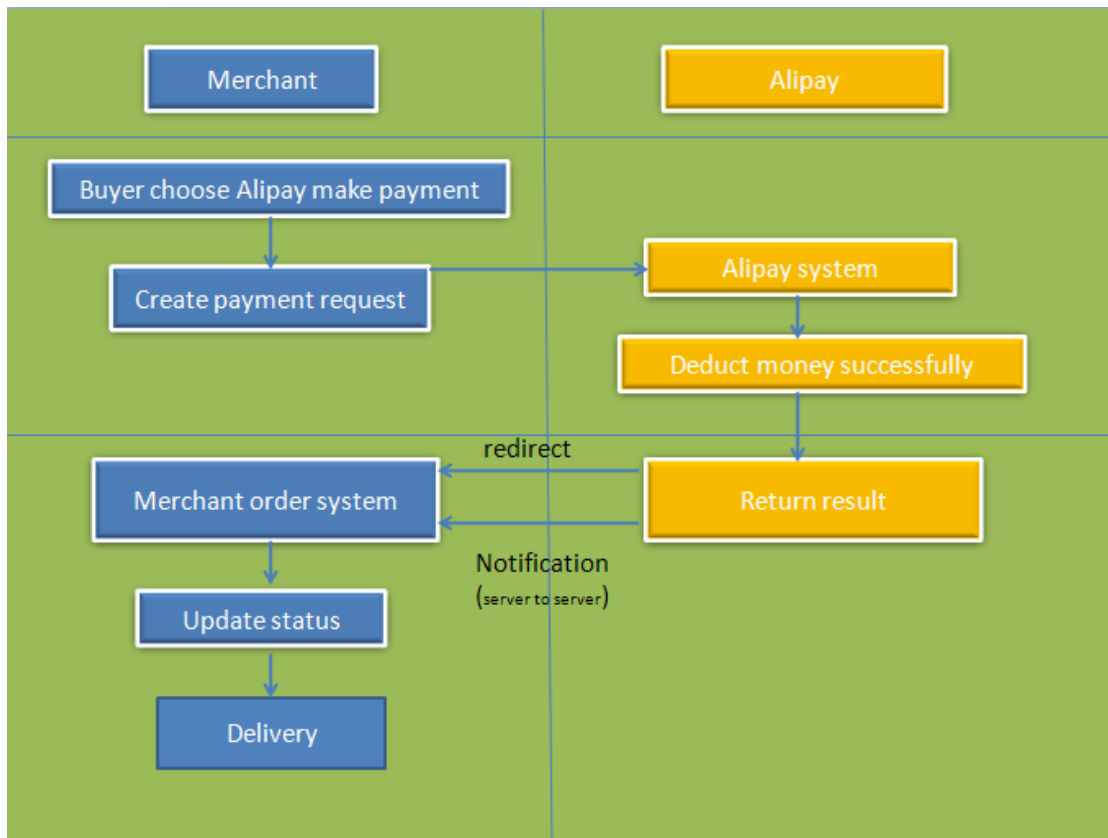
2.1. The Request/Respond Mode

The request/respond is the most frequently used interaction mode. Under the mode, the Merchant Partner System (partner system) sends request data to the Alipay Acquiring System (Alipay system), and synchronizely wait for the response from the Alipay system after the request has been processed.

The request/respond mode can be further classified into two types: *system invocation* and *page re-directed*. The system invocation type only needs to invoke the relevant API to perform the business operation, the page re-directed type on the other hand needs the operation to be done on the Alipay system's web page.

If the acquiring buyer completes the operation after being transferred to the Alipay's webpage, the Alipay system will return the results to the partner system's website, the user will continue the buying process on the partner's site. The parameter return_url (the next-step page url on the partner's website) for the must be specified
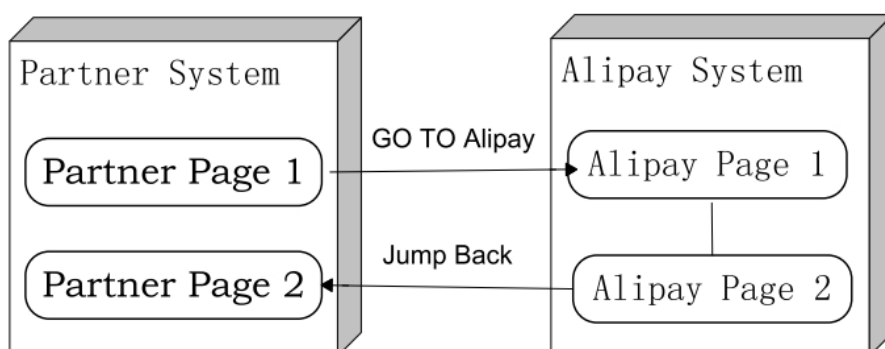
2.1.1. Process workflow
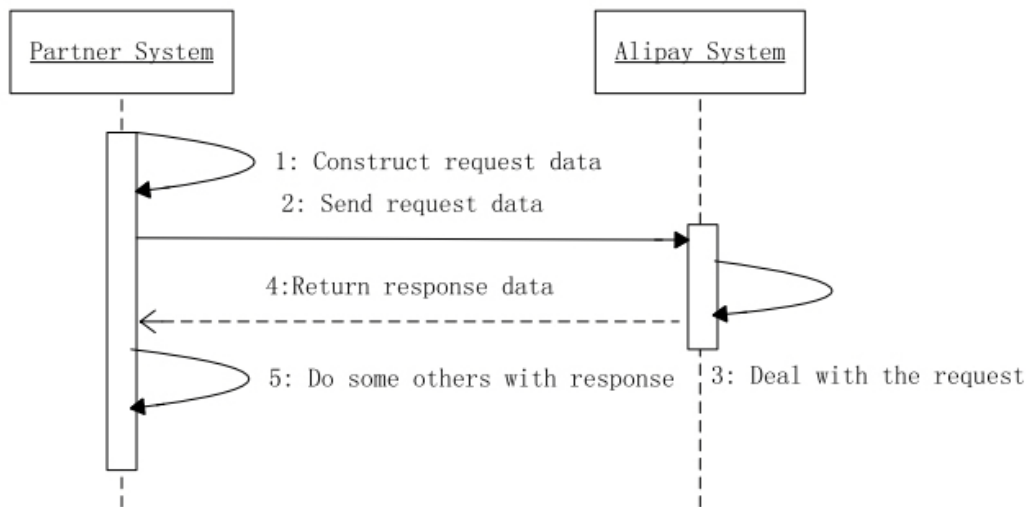
The gateway URL：

```
https://www.alipay.com/cooperate/gateway.do
```

2.2. Active Notifying Interaction Mode(server to server notification)

The acquiring buyer is sent to the Alipay's website from the partner's site. After completing the transaction, the buyer will not be sent back to the partner's site. Instead, the Alipay system will actively notify the partner's site on the buyer-related events.

If the session requires the result to be sent asynchronizely, the notify_url has be to specified， otherwise the parameter is not compulsory.

For example, a transaction has been created by the Partner system, when the transaction status (see: Transaction Status List) changes, the Alipay system sends the updated status and related information on the

transaction to the partner system.
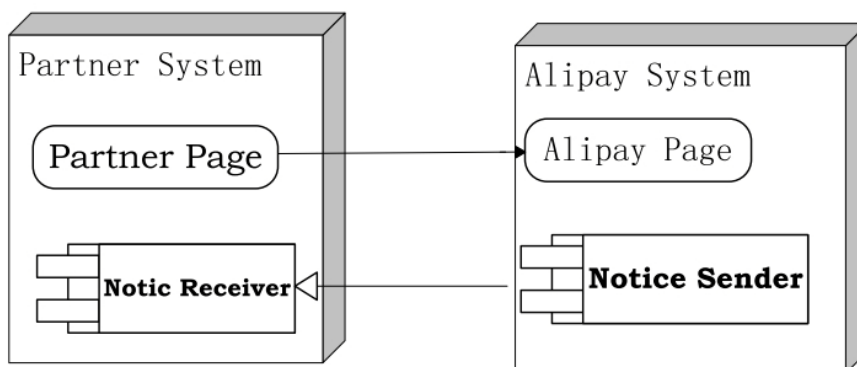
2.2.1. Process workflow
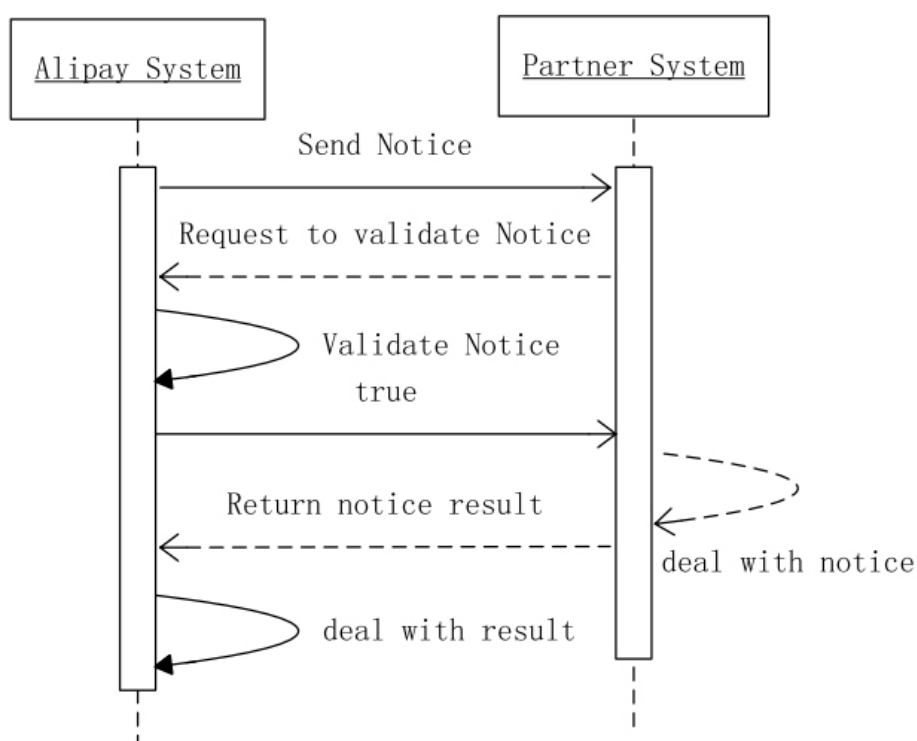
1. The Alipay system sends notification to the partner system, i.e. the URL for partner system to receive future notifications (the notify_url parameter)

2. The partner system receives the notification, sends back an authentication request with parameter notify_id to the Alipay system.

3. The Alipay system verifies the authentication, if genuine returns true, otherwise false.

4. Upon Alipay's confirmation, the partner system processes the request, and sends the result back to the Alipay's system.   The enumeration of the results can be found on the Appendix: Notification result list.

5. The Alipay system processes the notification result from the partner system.

The Alipay system delivers the data via HTTP/HTTPS POST method. The notify URL for the partner system can be configured statically in the API protocol, or it can be specified during each session dynamically via the notify_url parameter, e.g. if the notify_url is provided in the transaction creation request, all the future notification on this transaction will be sent through the specified notify_url from Alipay system to the partner system.

If the Alipay system fails to deliver the notification data, or the merchandise system fail to respond, the billing system will actively retry according to a prescribed schedule to maximize the delivery success rate, however it is not guaranteed all the active notification will be eventually delivered.

Due to this active notification mechanism, same notification can be sent multiple times to the partner system. Further, some ordered event active notification can be received asynchronizely with different order. Therefore the partner system must be able to ignore repeated notification and re-order the notifications. It is recommended by Alipay that upon receiving a notification, verification with relevant local data should be performed to determine if the notification has been already processed. The partner system is also expected to actively verify the correctness of notification order before processing the request, by data lock or time stamping to manage the concurrency.

2.2.2. Notification Verification

It is necessary for the partner system to verify the integrity and correctness of Alipay's notification. In the interest of system's healthiness, it is strongly recommended that the partner system apply such verification mechanism.

In order to guarantee the interface will be used legally, the partner system can only verify the notifications within the last 1 minute (this configuration is subject to change, and such change will not be notified).

The parameters：

Name	Parameter	Type	Description	Optional
Service Name	service	String	notify_verify.	N
The partner system	partner	String(16)	The ID of the partner on the Alipay system.	N
Notify ID	notify_id	String	The ID of Alipay system's notification.	N

✧ HTTPS-based notification verification interface

The program sends a HTTPS request according to the specification, and receives the response once the request has been completed. The possible outcome of the response is enumerated in the Output Result List. In order to use this interface, the HTTPS protocol must be supported by the website, otherwise HTTP-based notification verification interface should be used.

Gateway URL：

https://www.alipay.com/cooperate/gateway.do

An example of notification verification request:

```
https://www.alipay.com/cooperate/gateway.do?service=notify_ve
rify&partner=1234567890&notify_id=abcdefghijklmnopqrst
```

✧ HTTP-based notification verification interface

The program sends a HTTP request according to the specification, and receives the response once the request has been completed. The possible outcome of the response is enumerated in the Output Result List.

Gateway URL：

http://notify.alipay.com/trade/notify_query.do

An example of notification verification request:

```
http://notify.alipay.com/trade/notify_query.do?partner=123456
7890&notify_id=abcdefghijklmnopqrst
```

notification verification output result list：

Output result	Description
Invalid	The input parameter is invalid.
True	Authentication passed.
False	Authentication failed.

3. Security Standards

3.1. Digital Signature

To ensure the authenticity and the integrity of the data during transmission, the data needs to be accompanied by its digital signature, and the signature is used to verify the data.

3.1.1. The signature mechanism

A set of unsigned data is formatted as:

✧ The request parameters are sorted alphabetically in ascending order. If there is repeated parameter name, the repeated parameter is sorted according to the parameter value.

✧ All the parameters, (excluding `sign` and `sign_type`) are concatenated according the order with &. e.g: `p1=v1&p2=v2`.

If the following parameters require to be signed,

`service=user_query, partner=20880063000, email=test@msn.com`

Then the correct format before signing is:

`email=test@msn.com&partner=20880063000&service=user_query`

Notice:

✧ Parameters without value should be excluded.

✧ The characters should be encoded according to data stream's character set, specified in `_input_charset`.

✧ The `_input_charset` should be included in the data if required.

✧ According to HTTP requirement, if the characters in the parameter value includes special characters such as '&'、'@', the value

should be URL encoded to ensure the receiving end can decode the data correctly. In this case, the data to be signed is the data before URL encoding is performed. E.g. a request needs to specify user's email address, the data to be signed should be ：`email=test@msn.com`, instead of `email=test%40msn.com`。

3.1.2. Signature type

The signature is generated according to certain algorithm specified by parameter `sign_type`. (See ：Signature and encryption algorithm list)

4. Interface.

4.1. The payment interface

4.1.1. Business function

Once a buyer makes the payment through the alipay interface, it will redirect the buyer to the Alipay cashing page, where the buy have 3 options to make payment. The first choice is to deduct money from Alipay account balance. The second is to pay it through the bank account. And the last one is using Cartoon.

4.1.2. Interaction Mode

Request/Respond mode, Page re-directed type.
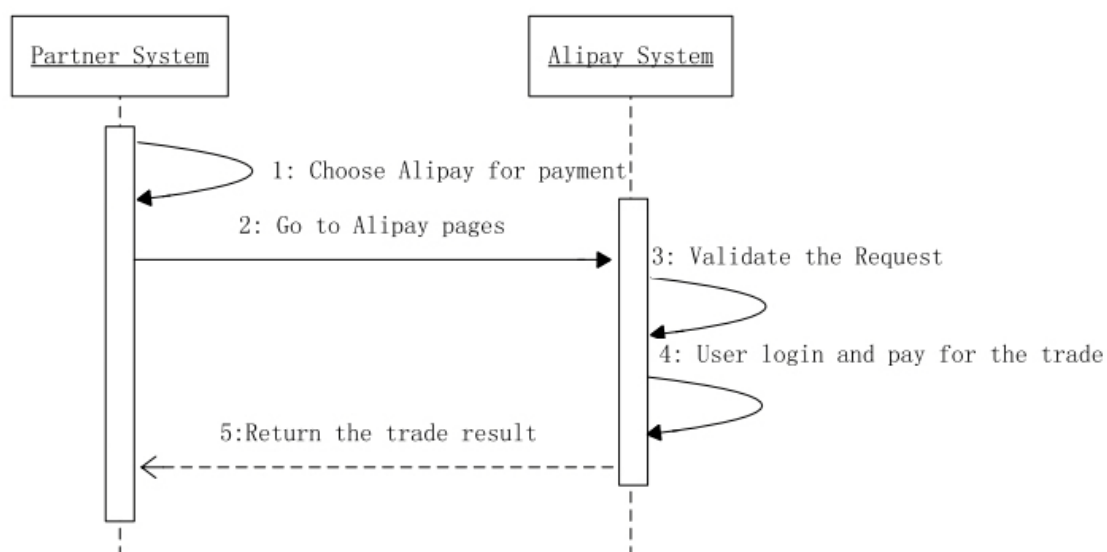
4.1.3. Request Parameters

Name	Parameter	Type	Description	Optional
Protocol Parameter				
Interface Name	service	String	create_direct_pay_by_user	N
Partner ID	partner	String(16)	Partner ID in Alipay system	N
Notify URL	notify_url	URL	Synchronize notify to receive URL according to Trade status	N
Return URL	return_url	URL	Result-return URL, only apply to those instant-return interface. Alipay return the Trade treatment result to this URL immediately after finishing the application	N
Signature	sign	String	Re. Signature Mechanism	N
Signature Method	sign_type	String	See: Signature mechanism	N
Goods Name	subject	String(256)		N
Goods Description	body	String(400)		Y
Out Trade No.	out_trade_no	String(64)	Partner Trade No.（Unique No. within partner system）	N
Total Trade Fee	total_fee	Number(8,2)	0.01 ～ 1000000.00 (RMB). The upper limit is lie on the instant trading fee limit on both side	N
Unit Price	price	Number(13,2)	0.01～100000000.00 (RMB)	N
Order Quantity	quantity	Number(6,0)	>0	N
Payment Type	payment_type	String	1	N
Default payment method	paymethod	String	bankPay; cartoon; directPay	Y
Default bankPay	defaultbank	String	Re. Bank List	Y

Seller Email	seller_email	String(100)	The seller's registered Email or registered ID. (Alternative Field)	N
Seller ID	seller_id	String(30)		
Royalty Type	royalty_type	String(2)	Current only one type available: Buyer give Commission to the third party (10)	
Royalty Parameters	royalty_parameters	String(500)	Account1 1^commission fee 1^Description 1|account2^commission fee2^Description2| account3^commission fee3^Description3 Maxim 5 accounts at a time. Description filed must within 30 bytes and without ^和|	

PS two way to pass the price ：

(1)Total Trade Volume: transfer the total_fee，neglect the price and quantity。
(2)unit price, quantity: transfer the price, quantity, neglect the total_fee。

Example of using royalty parameters：

In one trade, buyer need give commission to the third party, the input/output parameters are as below：

&royalty_type=10&royalty_parameters=hong_gr1%40alipay.com%5E10.20%5E%B8%F8%D0%A1%B7%D1%7Chong_gs1%40alipay.com%5E8.3%5E%B8%F8%BB%D8%BF%DB%7Chong_gr2%40alipay.com%5E0.5%5E%B8%F8%CC%E1%B3%C9

(%40 is @，%5E is ^，%7C is |)

Attention：The request parameters can only be accepted by the Alipay system

if they are signed according to the signature mechanism specified in this

document.

A full payment request example:

```
https://www.alipay.com/cooperate/gateway.do?_input_charset=utf-8&
body=%E5%95%86%E5%93%81%E6%8F%8F%E8%BF%B0&notify_url=http%3A%2F%2
Ftest%2Fphp%2Fnotify_url.php&out_trade_no=20090424040408&partner=
2088002509209142&payment_type=1&return_url=http%3A%2F%2Ftest%2Fph
p%2Freturn_url.php&royalty_parameters=tanlia_1988%40163.com%5E0.0
1%5E%E5%A5%96%E5%8A%B1%7Cming.yuhm%40alipay.com%5E0.01%5E%E5%A5%9
6%E5%8A%B1&royalty_type=10&seller_email=qibian1017%40hotmail.com&
service=create_direct_pay_by_user&show_url=http%3A%2F%2Ftest%2Fs
ubject=%E5%95%86%E5%93%81%E5%90%8D%E7%A7%B0&total_fee=0.03&sign=4
6ecf7fd8ea61548d5ba345a1512225f&sign_type=MD5
```

Output parameter

Name	Parameter	Type	Description	Optional
Protocol Parameter				
Notify Type	notify_type	String	trade_status_sync	N
Notify ID	notify_id	String	Alipay serial notify number, partner can use this number to verify the notification.	N
Notify Time	notify_time	Timestamp	Notify time（Alipay Time）, format： YYYY-MM-DD hh:mm:ss	N
Signature	sign	String	Re. HTTP parameter signature mechanism	N
Signature Method	sign_type	String	See: Signature mechanism	N
Alipay Trade No.	trade_no	String(64)	The Serial number for this trade in Alipay system	N
Out trade No.	out_trade_no	String(64)	The Serial number for this trade in Partner system	N
Payment Type	payment_type	String	1	N
Goods Name	subject	String(256)		N
Goods Description	body	String(400)		Y
Unit Price	price	Number(13,2)	0.01～100000000.00 (RMB)	N
Order Quantity	quantity	Number(6,0)	>0	N
Total Trade Fee	total_fee	Number(13,2)	0.01～1000000.00 (RMB)	N
Trade Status	trade_status	String	See : Transaction Status List	N

Seller's Email	seller_email	String(100)		N
Sell's ID	seller_id	String(30)		N
Buyer's ID	buyer_id	String(30)		N
Buyer's Email	buyer_email	String(100)		N

A full return url example:

```
http://test/php/return_url.php?body=%E5%95%86%E5%93%81%E6%8F%8F%E
8%BF%B0&buyer_email=tanlia1988%40163.com&buyer_id=208800264894945
5&exterface=create_direct_pay_by_user&is_success=T&notify_id=RqPn
CoPT3K9%252Fvwbh3I%252BI13%252BGXCeISaMKSka%252F90pTkqJMp74XKv46U
0mYgf1aQuWUD%252BMl&notify_time=2009-04-24+12%3A40%3A55&notify_ty
pe=trade_status_sync&out_trade_no=20090424040408&payment_type=1&s
eller_email=qibian1017%40hotmail.com&seller_id=2088002012489413&s
ubject=%E5%95%86%E5%93%81%E5%90%8D%E7%A7%B0&total_fee=0.03&trade_
no=2009042451140445&trade_status=TRADE_FINISHED&sign=206f8bd20203
35b10230f77852cca006&sign_type=MD5
```

Error response list

error_code	Description
ILLEGAL_SIGN	Illegal signature
ILLEGAL_ARGUMENT	Illegal parameters
HASH_NO_PRIVILEGE	No sufficient rights to complete the query
ILLEGAL_SERVICE	Service Parameter is incorrect
ILLEGAL_PARTNER	Incorrect Partner ID
ILLEGAL_SIGN_TYPE	Signature is of wrong type.
ILLEGAL_CHARSET	Illegal charset

Alipay's Notification Parameters

Name	Parameter	Type	Description	Optional
Protocol Parameters				
Notification type	notify_type	String	Notification type, value : trade_status_sync.	N
Notification ID	notify_id	String	The ID for a particular notification. It can be used by the partner system to verify the notification	N
Notification time	notify_time	Timestamp	Time (Alipay's time zone) : YYYY-MM-DD hh:mm:ss	N
Signature	sign	String	See: Signature mechanism	N
Signature Type	sign_type	String	See: Signature type	N
Business Parameters				
Partner transaction ID	out_trade_no	String(64)	A numbered transaction ID （Unique inside the partner system）	N

Status	trade_status	String(32)	See : Transaction Status List	N
Transaction ID	trade_no	String(16)	The transaction ID on the Alipay system	N
Discount	discount	Number(13, 2)		N
Payment type	payment_type	String(4)	1	N
Goods name	subject	String(256)		N
Unit price	price	Number(13, 2)	0.01～100000000.00	N
Quantity	quantity	Number(6,0)	>0	N
Time of creation	gmt_create	Timestamp	The time of payment is created	N
Buyer email	buyer_email	String(100)	Buyer Alipay account	N
Buyer ID	buyer_id	String(30)	Buyer id number	N
Seller email	seller_email	String(100)	Merchant's Alipay account	N
Seller ID	seller_id	String(30)	Merchant id	N
Time of payment	gmt_payment	Timestamp	the time of payment is made	N
Adjust amount	is_total_fee_adjust	String(1)	if the payment amount is adjusted	N
Coupon	use_coupon	String(1)	if coupon used	N
Goods description	body	String(400)	Goods description	N
Total trade fee	total_fee	Number(8 ,2)	Range: 0.01～1000000.00	N

A full notification example:

```
http://test/php/Notify_url.php?discount=0.00&payment_type=1&subje
ct=subject&trade_no=2009042451140445&buyer_email=tanlia1988@163.c
om&notify_type=trade_status_sync&gmt_create=2009-04-24
```

```
12:40:54&quantity=1&out_trade_no=20090424040408&notify_time=2009-
04-24
12:44:06&seller_id=2088002012489413&body=body&trade_status=TRADE_
FINISHED&is_total_fee_adjust=N&total_fee=0.03&gmt_payment=2009-04
-24
12:40:55&seller_email=qibian1017@hotmail.com&price=0.03&buyer_id=
2088002648949455&notify_id=841344847f078ff27850a80f4f9dce0e&use_c
oupon=N&sign_type=MD5&sign=235581ffe0546c3bdc3e71c957bca744
```

4.1.4. Alipay's response

After the Alipay system completed processing the request, the response will also have the sign and sign_type parameters. The partner system calculates the sign value according to the sign_type, and verifies the sign value that Alipay system returned. It should be noted that the partner system will need to decode the parameter values before checking the signature.

5. Appendix

5.1. Notification Result List

Result	Description
Success	Delivery successful, notification terminates.
Fail	Delivery failed, retry.

5.2. Bank list

Abbreviation	Bank
ICBCB2C	Industry and Commercial Bank of China
CMB	China Merchants Bank
CCB	Construction Bank of China
ABC	Agricultural Bank of China
SPDB	Shanghai Pudong Development Bank
SPDBB2B	Shanghai Pudong Development Bank (B2B)
CIB	China Industrial Bank
GDB	Guangdong Development Bank
SDB	Shenzhen Development Bank Co., Ltd.
CMBC	China Minsheng Banking Corp., Ltd.
COMM	Bank of Communications
POSTGC	Postal Savings Bank of China
CITIC	China Citic Bank
CCBVISA	Construction Bank of China VISA
VISA	VISA

5.3. Transaction Status List

Status	Description
WAIT_BUYER_PAY	The buyer is expected to make the payment
TRADE_FINISHED	The payment has been made, transaction closes.
TRADE_CLOSED	Transaction closed without payment.

5.4. Signature and Encryption Algorithms

5.4.1. Signature algorithms

Algorithm Function	MD5	DSA	RSA
Integrity check	√	√	√
Authentication	×	√	√
Encryption	×	×	√
Legal recognition	×	√	√

5.4.2. MD5 Signature

As a simple hashing digest function, the MD5 was not originally designed to be a signature generation algorithm; however, by appending the key (a common key known both to the sender and the receiver) into the data, the MD5 sum can be used as a form of digital signature.

For example, if the key is set to be :32#af*dsf, the partner system's request should be formatted as:

```
email=test@msn.com&service=user_query32#af*dsf
```

However such scheme can only detect if the data has been modified or not. Due to the key is known to both sender and receiver; it cannot be used to authenticate the sender.

5.4.3. DSA Signature

DSA is an asymmetric signature generation algorithm. Asymmetric means the signature key (the private key) and the verification key (public key) is different. Therefore the signature not only can be used in attack detection but it can also be used to authenticate the sender, since the private key is only known to the sender.

When the partner system sends a request, it can use its own private key

to generate a DSA signature. Once the request has been received, the Alipay system can verify the signature using the public key provided by the partner. The Alipay generates the respond signature using its own private key; vice versa the signature can be verified by the partner using the public key provided by Alipay.

5.4.4. RSA Signature

RSA is also an asymmetric signature generation algorithm, similar to the DSA algorithm, however encryption is cooperated in RSA to enhance the security measure.

5.5. OpenSSL

5.5.1. DSA Key Generation

1. Generating DSA parameters
```
openssl dsaparam -out dsa_param.pem 1024
```

2. Generating DSA private key
```
openssl gendsa -out dsa_private_key.pem dsa_param.pem
```

3. Generating DSA public key
```
openssl dsa -in dsa_private_key.pem -pubout -out dsa_public_key.pem
```

4. Converting DSA private key into PKCS8 format
```
openssl pkcs8 -topk8 -inform PEM -in dsa_private_key.pem -outform PEM
-nocrypt
```

5.5.2. RSA Key Generation

1. Generating RSA private key
```
openssl genrsa -out rsa_private_key.pem 1024
```

2. Generating RSA public key
```
openssl rsa -in rsa_private_key.pem -pubout -out rsa_public_key.pem
```

3. Converting RSA private key into PKCS8
```
openssl pkcs8 -topk8 -inform PEM -in rsa_private_key.pem -outform PEM
-nocrypt
```

5.5.3. Signature verification

✧ RSA Signing:

```
openssl sha1 -sign rsa_private_key.pem -out rsasign.bin plaintext.txt
```

✧ RSA Signature verification

```
openssl sha1 -verify rsa_public_key.pem -signature rsasign.bin
plaintext.txt
```

✧ DSA Signing

```
openssl dgst -dss1 -sign dsa_private_key.pem -out dsasign.bin
plaintext.txt
```

✧ DSA verification

```
openssl dgst -dss1 -verify dsa_public_key.pem -signature dsasign.bin
plaintext.txt
```

Base64 Encoding on the signature:

```
openssl base64 -in rsasign.bin -out base64.txt
```

Base64 Decoding on the signature:

```
openssl base64 -d -in base64.txt -out rsasign.bin
```