Triple Check API

Forte Payment Systems

Revised August 8, 2013

Table of Contents

Overview

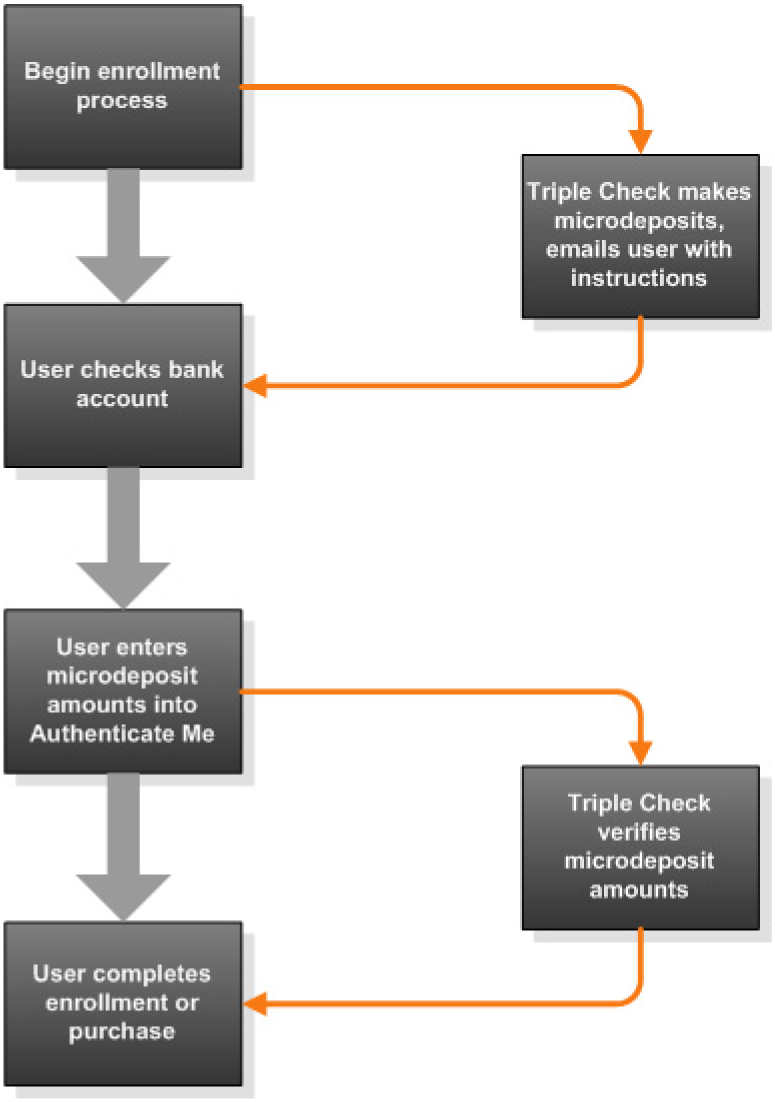
Triple Check is a web service that allows you to verify a consumer's bank account before enabling purchases or recurring payments. Triple Check has two functions that allow you to do this:

- **Account Verification** - Triple Check verifies the account information provided by the consumer against risk and negative databases to provide an approved or declined response based on the account's history.
- **Micro-deposits** - Triple Check initiates three micro-deposits to the consumer's bank account and requires the consumer to verify the amounts using the Authenticate Me site (www.authenticateme.com). This verifies that the consumer has access to the account.

Triple Check can be integrated into your application using our RESTful web service.

Consumer Flow

From the consumer's standpoint, the Triple Check process is as follows:


Begin enrollment process
Triple Check makes microdeposits, emails user with instructions
User checks bank account
User enters microdeposit amounts into Authenticate Me
Triple Check verifies microdeposit amounts
User completes enrollment or purchase

1. The consumer begins the enrollment process on the merchant website. The consumer enters the email account and bank account information for the account he/she wishes to link.
2. The merchant initiates the Triple Check process and Triple Check initiates three micro-deposits to the consumer's account. The micro-deposits will be viewable to the consumer in one to two business days.

An email is sent to the consumer at the specified email address with instructions for verifying the micro-deposits. The following is a sample verification email:

Dear John Doe,

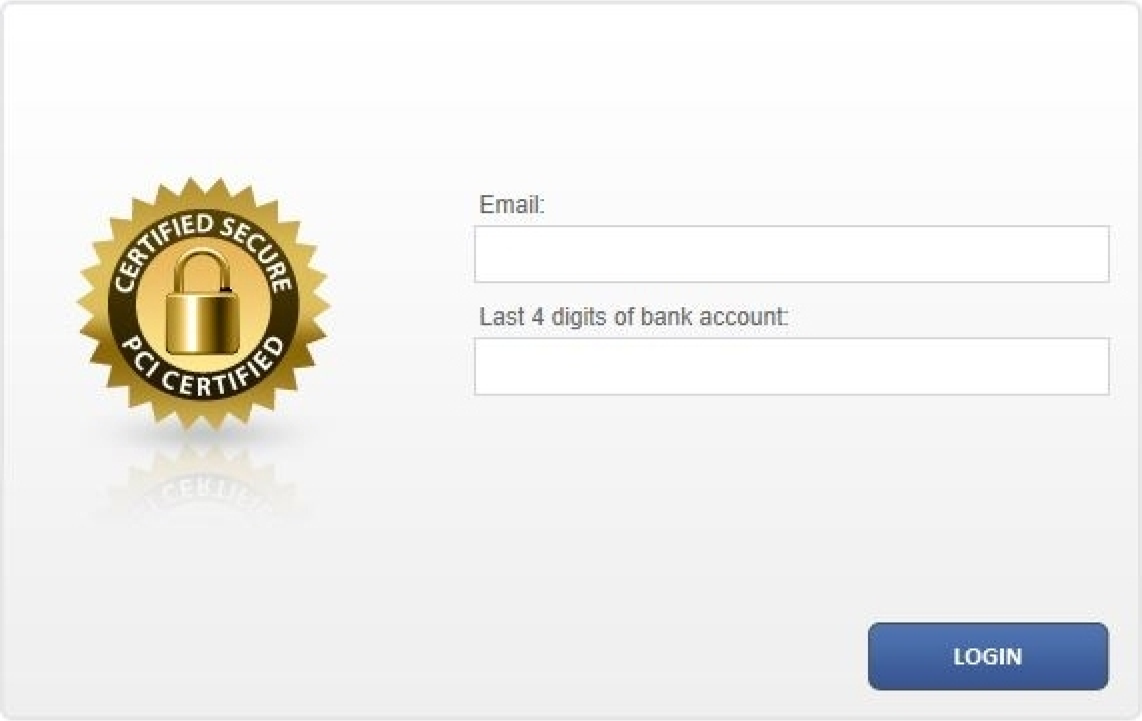
Thank you for applying with ABC Company. In order to proceed with your order, you need to authenticate your account. Please do so by going to www.authenticateme.com, enter your email address and the last four digits of your account number. Then enter the amounts of the debits and credits that were generated against your account.

Thank you,

ABC Co, Inc.
1234 Any Street
Anytown, Texas 75013
www.abcco.com

3. The consumer checks his account to view the values of the micro-deposits.
4. The consumer follows the instructions in the verification email and enters the values of the micro-deposits on the Authenticate Me site (www.authenticateme.com).

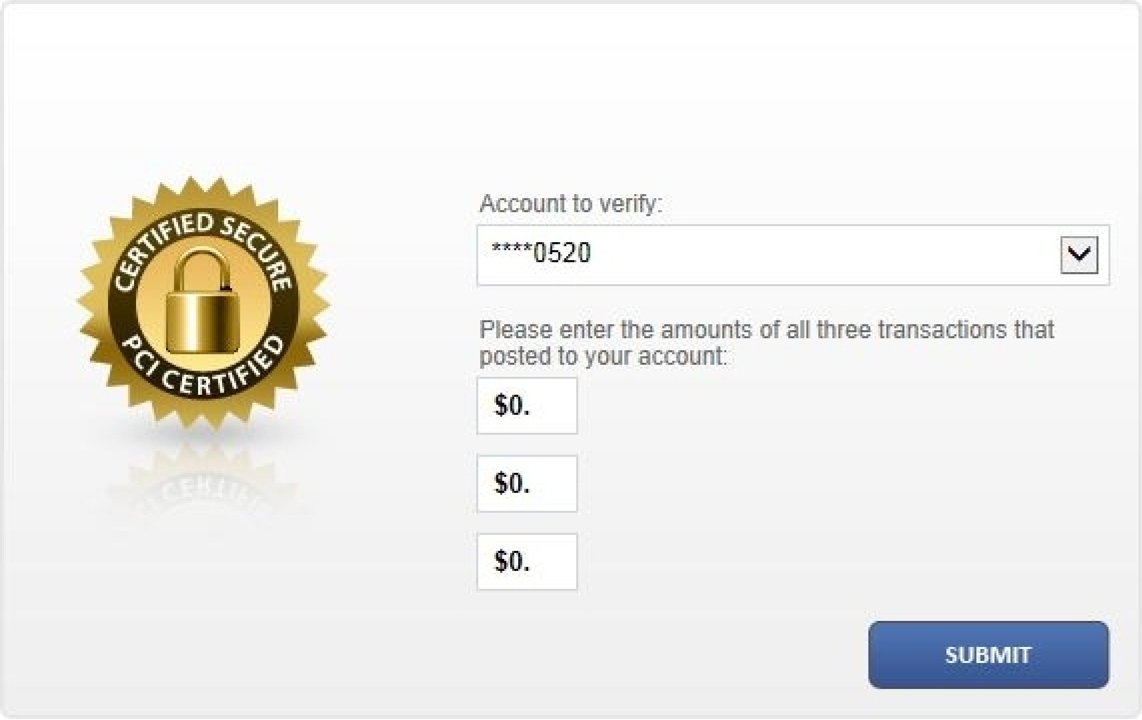
   The following shows the log in screen for the Authenticate Me site:



Email:

Last 4 digits of bank account:

The following shows the deposit verification screen for the Authenticate Me site:



Account to verify:

****0520

Please enter the amounts of all three transactions that posted to your account:

$0.

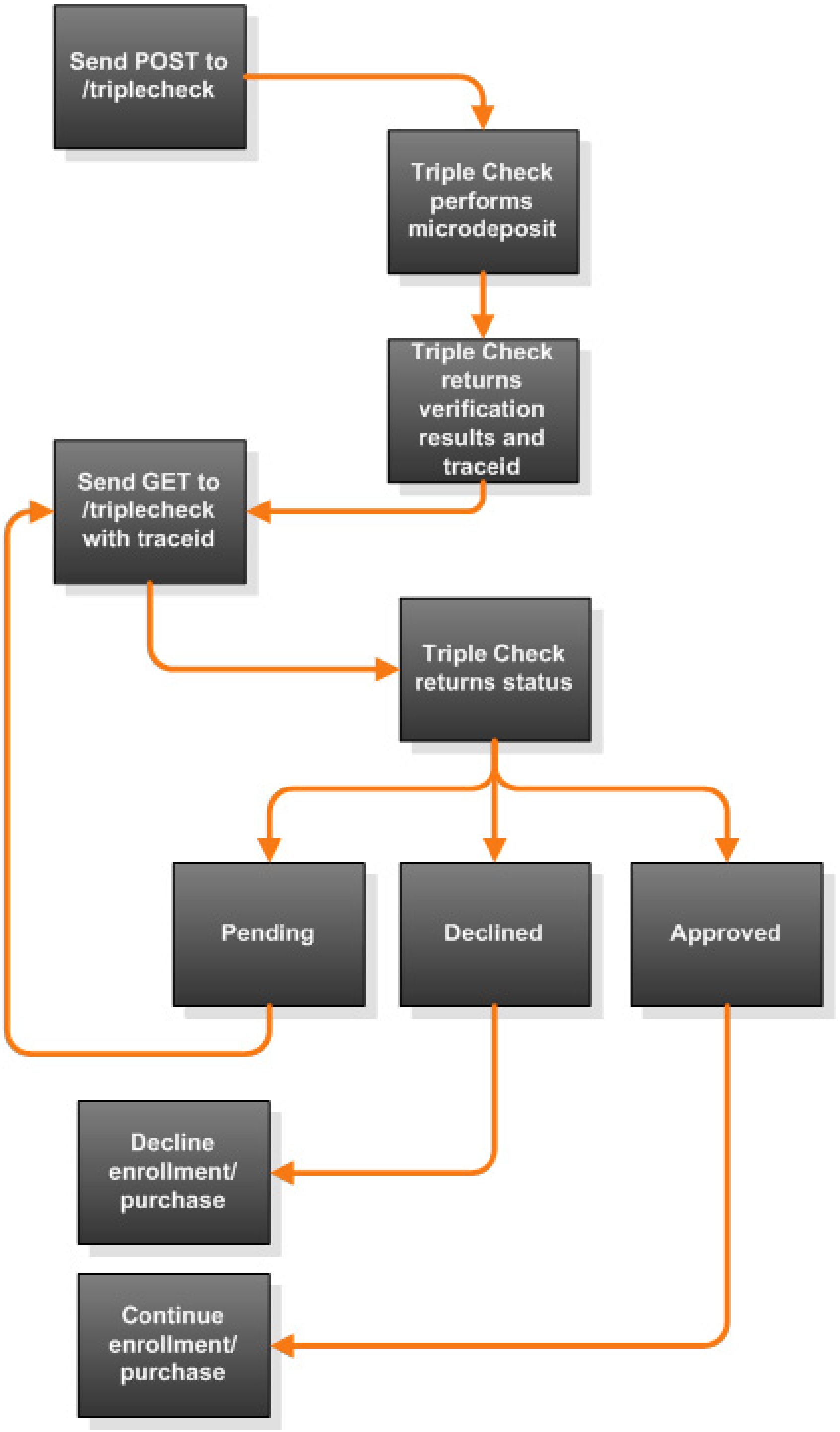
$0.

$0.

5. Once the micro-deposits have been verified, the merchant provides the user with instructions on how to complete the enrollment or purchase.

Application Flow

The following shows the process the application must complete to verify the consumer's account:


Send POST to /triplecheck
Triple Check performs microdeposit
Triple Check returns verification results and traceid
Send GET to /triplecheck with traceid
Triple Check returns status
Pending
Declined
Approved
Decline enrollment/ purchase
Continue enrollment/ purchase

1. After the consumer initiates the enrollment or purchase and enters his bank account information, the merchant sends a POST to /triplecheck with the consumer's account information.
2. Triple Check makes the micro-deposit and credit to the consumer's account, emails the consumer with instructions to verify the amount, and returns a traceid value to the merchant website. Triple Check also returns an account verification response.
3. The merchant periodically polls Triple Check by sending a GET to /triplecheck with the traceid value returned in the POST response.
4. Triple Check returns a value indicating if the micro-deposits have correctly verified, incorrectly entered, or still pending.
5. If the micro-deposits are still pending, the merchant continues to perdiodically poll Triple Check by sending a GET to /triplecheck with the traceid value returned in the post response.
6. If the micro-deposit amounts are entered incorrectly three times, the process is complete and the merchant website can decline enrollment or purchase using the entered bank account information.
7. If the micro-deposit amounts are entered correctly, the process is complete and the merchant website can continue the purchase or enrolmment process.

Authentication

Generating an API Login ID and Secure Transaction Key

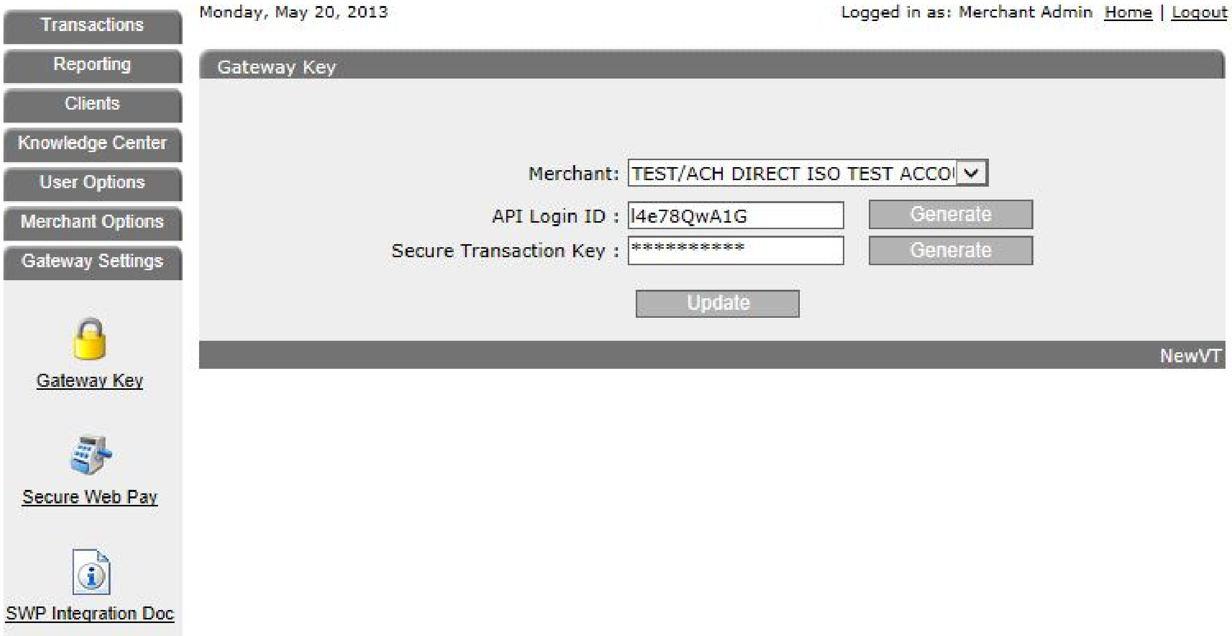
Before sending messages to the Triple Check service, you must generate your API login ID and Secure Transaction Key values which are required for authentication. You must have a merchant account with Forte to generate these values. If you don't have a Forte account yet, please call us at 866-290-5400 Option 3.

To generate an API login ID and Secure Transaction Key, follow these steps:

1. Log in to your account at:

   www.paymentsgateway.net

2. Click the **Gateway Settings** tab.
3. Click **Gateway Key** under **Gateway Settings**.
4. The following screen displays:



Monday, May 20, 2013

Logged in as: Merchant Admin

Merchant: TEST/ACH DIRECT ISO TEST ACCO

API Login ID : l4e78QwA1G

Secure Transaction Key : ***********

5. Click **Generate** next to API Login ID to generate a new value.

   Click **Generate** next to Secure Transaction Key to generate a new value.

   Record these values for use in authentication.

6. Click **Update** to save these values.

   Note: Once you click update, you will not be able to see these values again.

Computing the Authentication Hash

The following fields are sent in each request message for authentication with the Triple Check service:

Parameter	Required	Description
hash_method	No	The method used to hash the authentication value in the ts_hash field. The default value is MD5. Possible values are: • **MD5** - HMAC-MD5 • **SHA1** - HMAC-SHA1 • **SHA256** - HMAC-SHA256
ts_hash	Yes	The computed authentication hash value. See below for instructions on computing the authentication hash value.
utc_time	Yes	UTC time in system ticks since 01/01/0001 00:00:00.
api_login_id	Yes	Your API login ID.

The ts_hash value is computed using the authentication fields described above along with the Secure Transaction Key.

To compute the hash, first concatenate the following values:

```
api_login_id + "|" + HTTP verb (POST or GET) + "|" +
"TripleCheck" + "|" + utc_time
```

Then compute the HMAC hash using the method identified in the hash_method field with the Secure Transaction Key as the key value.

For example, when sending a POST request as api_login_id xyz987654 at 635044211106270000 UTC time and using MD5 as the hash_method, and the Secret Transaction Key is XYZ98786abcd99, the application should calculate the following value:

```
HMAC-MD5("xyz987654|POST|TripleCheck|635044211106270000",
"XYZ98786abcd99")
```

Perform Account Check

Sending a POST to Triple Check initiates an account check.

Request

POST `https://ws.paymentsgateway.net/triplecheck/v1/`

Send the following values as POST parameters to the triplecheck endpoint:

Parameter	Required	Description
check_trn	Yes	The routing number of the consumer's bank account to verify. Up to 9 numeric digits.
check_account	Yes	The account number of the consumer's bank account to verify. Up to 18 numeric digits.
email_address	Yes	The email address of the consumer account holder. This is the email address at which the consumer receives the instructions to verify the micro-deposit amounts. Up to 40 alphanumeric characters.
company_name	Required for business accounts	The company name of the consumer account holder. Required if for business accounts (owner_account_type is B). Up to 40 alphanumeric characters.
account_signer_prefix	No	Name prefix of the consumer account holder. Up to 3 alphanumeric characters.
account_signer_first_name	Yes	First name of the consumer account holder. Up to 20 alphanumeric characters.
account_signer_middle_name	No	Middle name of the consumer account holder. Up to 20 alphanumeric characters.
account_signer_last_name	Yes	Last name of the consumer account holder. Up to 20 alphanumeric characters.

Parameter	Required	Description
account_signer_name_suffix	No	Name suffix of the consumer account holder. Up to 3 alphanumeric characters.
account_holder_address	No	First line of the consumer account holder's address. Up to 20 alphanumeric characters.
account_holder_address2	No	Second line of the consumer account holder's address. Up to 20 alphanumeric characters.
account_holder_city	No	City of the consumer account holder's address. Up to 20 alphanumeric characters.
account_holder_state	No	Two alphanumeric digit state code of the consumer account holder's address.
account_holder_postal_code	No	ZIP/postal code of the consumer account holder's address. Up to 10 alphanumeric characters.
account_holder_home_phone	No	Home phone of the consumer account holder. Up to 10 numeric digits.
account_holder_work_phone	No	Work phone of the consumer account holder. Up to 10 numeric digits.
account_holder_drivers_lic	No	Driver's license number of the consumer account holder. Up to 28 alphanumeric characters.
account_holder_drivers_lic_state	No	Two alphanumeric digit state code from the consumer account holder's driver's license.
account_holder_drivers_lic_dob	No	Date of birth from the consumer account holder's driver's license in MMddyyyy format.
consumer_indicator	Yes	Indicates if the consumer is present at the time of the transaction. Possible values are: • **P** - The consumer is present. • **N** - The consumer is not present.

Parameter	Required	Description
enrollment_indicator	Yes	Indicates if the transaction involves the consumer enrolling in a service or making a purchase. Possible values are: • **E** - Enrollment transaction • **P** - Purchase transaction
tax_id_ssn	No	Federal tax ID or Social Security Number of the consumer account holder. 9 numeric digits.
check_number	No	The check number from the consumer's check. Up to 15 numeric digits.
owner_account_type	Yes	Indicates if the consumer's account is business or personal. Possible values are: • **B** - Business • **P** - Personal
check_account_type	Yes	Indicates if the consumer's account is checking or savings. Possible values are: • **C** - Checking • **S** - Savings
amount	Required for purchase transactions	The amount of the transaction for purchase transactions. Required if for purchase transactions (enrollment_indicator is P). Up to 12 numeric digits, including decimal ($$$$$$$$$.cc format).
user_defined_field_1	No	Optional field that is echoed back to the merchant in the response message, such as consumer account number, policy number, or invoice number. Up to 15 alphanumeric characters.
user_defined_field_2	No	Optional field that is echoed back to the merchant in the response message, such as consumer account number, policy number, or invoice number. Up to 40 alphanumeric characters.

Parameter	Required	Description
user_defined_field_3	No	Optional field that is echoed back to the merchant in the response message, such as consumer account number, policy number, or invoice number. Up to 40 alphanumeric characters.
user_defined_field_4	No	Optional field that is echoed back to the merchant in the response message, such as consumer account number, policy number, or invoice number. Up to 40 alphanumeric characters.
hash_method	No	The method used to hash the authentication value in the ts_hash field. See Authentication for complete instructions on using the authentication fields. The default value is MD5. Possible values are: • **MD5** - HMAC-MD5 • **SHA1** - HMAC-SHA1 • **SHA256** - HMAC-SHA256
ts_hash	Yes	The computed authentication hash value. See Authentication for complete instructions on using the authentication fields.
utc_time	Yes	UTC time in system ticks since 01/01/0001. See Authentication for complete instructions on using the authentication fields.
api_login_id	Yes	Your API login ID. See Authentication for complete instructions on using the authentication fields.

POST Response

By default, Triple Check returns the response as JSON contained in a triplecheck object. To request XML, specifiy application/xml in the HTTP Accept header.

Triple Check responds with default HTTP response codes. See HTTP Response Codes for descriptions of response values.

The triplecheck object contains the following fields:

Parameter	Description
md_credit_status	The status of the credit micro-deposit to the consumer's account. Possible values are: • **V** - Validated - Entry amount has been validated by account owner • **P** - Pending - Micro-deposits have been requested or sent for this account combo • **F** - Failed - Amounts have not been validated by account owner and attempts to validate have been exhausted • **E** - Expired - Amounts have not been validated within the seven day limit • **R** - Returned - Micro-deposit entries were returned/did not post to the account • **D** - Deleted - One or more micro-deposits have been deleted
md_debit_status	The status of the debit micro-deposits to the consumer's account. Possible values are: • **V** - Validated - Entry amount has been validated by account owner • **P** - Pending - Micro-deposits have been requested or sent for this account combo • **F** - Failed - Amounts have not been validated by account owner and attempts to validate have been exhausted • **E** - Expired - Amounts have not been validated within the seven day limit • **R** - Returned - Micro-deposit entries were returned/did not post to the account • **D** - Deleted - One or more micro-deposits have been deleted

Parameter	Description
md_status	Overall micro-deposit status accounting for the one credit and two debit micro-deposits. Possible values are: • **G** - Good - Account verified; all micro-deposits are validated. • **B** - Bad - Account not verified; one or more micro-deposits were not validated • **U** - Unknown - Validation is still pending for one or more micro-deposit values
trace_id	The trace ID value used to get updates on the status of the Triple Check request using the GET method.
verification_result_description	A description of the result provided by the account verification service. Possible approval values are: • P40:NO NEG INFO • P50:NO INFO • P70:VALIDATED • P71:LOW RISK APPROVAL • P73:MEDIUM RISK APPROVAL • P80:PREAUTH VENDOR BUSY • P90:PREAUTH VENDOR UNAVAIL • P91:PREAUTH VENDOR ERROR • P92:PREAUTH SERVER UNAVAIL Possible decline values are: • P15:HIGH RISK • P41:NEGATIVE INFO • U02:TRN NOT APPROVED • U02:ACCOUNT NOT APPROVED • U19:INVALID TRN
verification_result_type	A one digit code describing the type of result provided by the account verification service. Possible values are: • **A** - Approved • **D** - Declined • **E** - Error

The following is a sample JSON response:

```
{"verification_result_type":"D",
  "verification_result_description":"P15:HIGH RISK",
  "md_credit_status":"P",
  "md_debit_status":"P",
  "md_status":"U",
  "trace_id":"wNfMEHcVREG3Pe-J6nYefA"}
```

The following is a sample XML response:

```
<triplecheck xmlns:i="http://www.w3.org/2001/XMLSchema-instance"
xmlns="http://schemas.datacontract.org/2004/07/TripleCheck.Model
s">
     <md_credit_status>P</md_credit_status>
     <md_debit_status>P</md_debit_status>
     <md_status>U</md_status>
     <trace_id>1VHYVvoZIk6_APEFM4wvsg</trace_id>
     <verification_result_description>P71:LOW RISK APPROVAL
 </verificaton_result_description>
     <verification_result_type>A</verificaton_result_type>
 </triplecheck>
```

Get Account Check Results

After submitting a POST to the triplecheck endpoint, poll the GET endpoint using the trace ID returned in the original POST response to get an update on the status of the micro-deposit verification process.

Request

GET `https://ws.paymentsgateway.net/triplecheck/v1/`

Send the following values as URL parameters to the triplecheck endpoint:

Parameter	Required	Description
trace_id	Yes	The alphanumeric trace_id value for the Triple Check initiation returned in the POST response.
hash_method	No	The method used to hash the authentication value in the ts_hash field. See Authentication for complete instructions on using the authentication fields. The default value is MD5. Possible values are: • **MD5** - HMAC-MD5 • **SHA1** - HMAC-SHA1 • **SHA256** - HMAC-SHA256
ts_hash	Yes	The computed authentication hash value. See Authentication for complete instructions on using the authentication fields.
utc_time	Yes	UTC time in system ticks since 01/01/0001. See Authentication for complete instructions on using the authentication fields.
api_login_id	Yes	Your API login ID. See Authentication for complete instructions on using the authentication fields.

The following is a sample request to the GET endpoint:

```
https://ws.paymentsgateway.net/triplecheck/v1/wNfMEHcVREG3Pe-
J6nYefA?hash_method=...&ts_hash=...&utc_time=…&api_login_id=…
```

GET Response

By default, Triple Check returns the response as JSON contained in a triplecheck object. To request XML, specifiy application/xml in the HTTP Accept header.

Triple Check responds with default HTTP response codes. See HTTP Response Codes for descriptions of response values.

The triplecheck object contains the following fields:

Parameter	Description
md_credit_status	The status of the credit micro-deposit to the consumer's account. Possible values are: • **V** - Validated - Entry amount has been validated by account owner • **P** - Pending - Micro-deposits have been requested or sent for this account combo • **F** - Failed - Amounts have not been validated by account owner and attempts to validate have been exhausted • **E** - Expired - Amounts have not been validated within the seven day limit • **R** - Returned - Micro-deposit entries were returned/did not post to the account • **D** - Deleted - One or more micro-deposits have been deleted
md_debit_status	The status of the debit micro-deposits to the consumer's account. Possible values are: • **V** - Validated - Entry amount has been validated by account owner • **P** - Pending - Micro-deposits have been requested or sent for this account combo • **F** - Failed - Amounts have not been validated by account owner and attempts to validate have been exhausted • **E** - Expired - Amounts have not been validated within the seven day limit • **R** - Returned - Micro-deposit entries were returned/did not post to the account • **D** - Deleted - One or more micro-deposits have been deleted

Parameter	Description
md_status	Overall micro-deposit status accounting for the one credit and two debit micro-deposits. Possible values are: • **G** - Good - Account verified; all micro-deposits are validated. • **B** - Bad - Account not verified; one or more micro-deposits were not validated • **U** - Unknown - Validation is still pending for one or more micro-deposit values
trace_id	The alphanumeric trace_id value for the Triple Check initiation returned in the POST response.
verification_result_type	A one digit code describing the type of result provided by the account verification service. Possible values are: • **A** - Approved • **D** - Declined • **E** - Error

The following is a sample JSON response:

```
{"verification_result_type":"D",
   "md_credit_status":"P",
   "md_debit_status":"P",
   "md_status":"U",
   "trace_id":"wNfMEHcVREG3Pe-J6nYefA"}
```

The following is a sample XML response:

```
<triplecheck xmlns:i="http://www.w3.org/2001/XMLSchema-instance"
xmlns="http://schemas.datacontract.org/2004/07/TripleCheck.Model
s">
     <md_credit_status>P</md_credit_status>
     <md_debit_status>P</md_debit_status>
     <md_status>U</md_status>
     <trace_id>1VHYVvoZIk6_APEFM4wvsg</trace_id>
     <verification_result_type>A</verificaton_result_type>
 </triplecheck>
```

HTTP Response Codes

Triple Check returns standard HTTP response codes with additional messages returned in JSON:

- **200** - OK
- **400** - Bad Request
- **401** - Unauthorized
- **402** - Request Failed
- **403** - Forbidden
- **404** - Not found
- **405** - Allowed
- **409** - Conflict
- **500** - Internal Server Error
- **503** - Service Unavailable

The following table describes the messages returned:

Response Code	Description	Message
400	Request does not include a host header.	n/a
400	Authentication is invalid .	n/a
400	Required field is not present.	{parameter name} is required.
400	Parameter length exceeded.	{parameter name} length exceeded.
400	Parameter expects certain type of character; for example, state is a number or enrollment_indicator is a number or not e or p.	{parameter name} is invalid.
400	Routing number does not pass checksum.	Routing number is invalid.
400	Email does not pass regular expression.	Email address is invalid.
400	Federal tax ID or SSN does not pass regular expression.	FederalTaxSSN is an invalid format.
400	State is not a valid state code, for example AA.	State is not valid.
405	Verb used incorrectly for a resource.	n/a