UGPAYMENTS – DIRECT 3D 2.0

TABLE OF CONTENTS

REVISION HISTORY

Date	Revision	Description	Author
6/8/2021	1	First Revision	Unicorn
12/3/2022	2	Added ConfirmURL	Unicorn
1/22/2024	3	Added Browser Data	Unicorn
7/26/2024	4	Removed Enrollment Status, always return Y, F	Unicorn
8/28/2024	5	Added new test cases, added void/capture/refund	Unicorn
12/20/2024	6	Added new test cases, clarified 3D Flow	Unicorn
2/27/2025	7	Added 2DS Fallback	Unicorn
4/9/2025	8	Corrected fallback flow	Unicorn
2/5/2026	9 – version 2.7	Updated test cases, made AuthType required field, added valid ColorDepth range	Unicorn
3/10/2026	10 – version2.8	Updated test cases	Unicorn
6/29/2026	11 – version 2.9	Updated rebill	Unicorn
8/19/2026	11 – version 3	Updated rebill fields	Unicorn
8/24/2026	12 – version 3.1	Added decline responses	Unicorn

OVERVIEW

WHAT IS 3-D SECURE 2.0

As the share of e-commerce and especially mobile transactions is growing, the industry has been suffering from high chargeback ratios and low approval ratios compared to card present transactions. With the introduction of 3D-Secure 2.0, this gap should be minimized.

The SCA mandate requires 3D-Secure to be applied to all electronic payments – including proximity, remote and mobile payments – within the European Economic Area (EEA). The strong customer authentication mandate is complemented by some limited exemptions that aim to support a frictionless customer experience when transaction risk is low.

3D-Secure 2.0 supports the transfer of rich data for transactions enabling possible risk-based decisions regarding whether to authenticate or not. This means that based on certain criteria, the end user may or may not be asked to perform a ‘challenge’ to
ensure their authenticity. The consumer experience has also been simplified and enhanced thanks to the elimination of the preliminary enrolment process and by not requiring the end user to remember as many passwords.

During the 3D-Secure 2.0 authentication, the issuer performs a risk-based analysis to determine whether a transaction should be challenged. A challenge means that the user is presented with an authentication screen of the issuer that follows the Strong Customer Authentication rules. Issuer risk analysis is performed based on the data collected during the transaction, such as device information, transaction information, time zone and various other parameters. If an issuer determines that the transaction is low risk, a frictionless indicator is returned in the authentication response. Frictionless flow means that the transaction is considered 3D authenticated and a liability shift applies, without the need of the user challenge screen.

It is highly recommended that merchants send as many optional parameters as possible during the authentication, as it increases the chance of frictionless flow and better user conversion.

REQUIRED INFORMATION

Before you will be able to submit transactions to UnicornGroup, you will need an UnicornGroup merchant account for your website. Once you have a merchant account established, UnicornGroup will supply you with:

1. Merchant Id
2. Site Id
3. OAuth Bearer Token

These IDs uniquely identify your websites, customers, and payments.

SOFTWARE REQUIREMENTS

To implement the JSON interface for standard card processing, the following requirements must be met:

- Working knowledge of JSON
- SSL server supporting 128-bit (or stronger) encryption

3-D SECURE2.0 PAYMENT AUTHENTICATION FLOW

Step 1 The cardholder shops at the merchant's website. At checkout, he/she enters the payment details (including credit card details) and clicks the purchase order button.

Step 2 The merchant sends the payment details to the Unicorn hosted Check Enrollment API through the endpoint /checkenrollment

Step 3 Unicorn verifies if the merchant is 3-D Secure enabled and if the cardholder (the card itself) is 3-D-enrolled, either 1.0 or 2.0. If the cardholder is enrolled, the Unicorn system returns an EnrollmentStatus of "Y" (Enrolled) or "F" (Challenge), and, the Unicorn system will then return an Access Control Server URL (Acsurl) to where the customer must be redirected by the merchant (Step 4).

If a card is not enrolled, you will get the following message:

3D transaction not permitted due to card bin is from outside of EEA states + UK. Fallback to the Non-3D transaction with no liability shifted.

In this case, you will then call the /ThreeDSaleTransactions or if you wish to authorize, /ThreeDAuthorizeTransactions endpoint by passing the VerifyTransactionID. It will then process payment as 2DS and no liability shift occurs.

Step 4 The merchant sends a HTTP POST request to the AcsUrl with the variables "AuthType", "transactionId", and "TermUrl". This TermUrl is the url on the merchant's site that the customer will be returned to once authentication is complete. See example below.

Example Form:

```
<form name="acs" method="post" action="<acsurl_value> ">
   <input name="transactionId" type="hidden" value="3605449" /><br />
   <input name="AuthType" type="hidden" value="doChallenge" />
   <input name="TermUrl" type="hidden" value="http://merchantssite.com/process3dsale.php" />
   <input type="submit" value="Authenticate ACS URL" />
</form>
```

Step 5 A return back to the TermURL will contain a variable Id which will be sent to the endpoint /ThreeDSaleTransaction as VerifyTransactionId to complete the sale.

****ONLY CALL /ThreeDSaleTransaction IF RESPONSE TO TERMURL IS SUCCESSFUL!****
****IF NO CALL TO /ThreeDSaleTransaction IS COMPLETED, THERE IS NO SALE****

Please note, customer MAY close the browser during this redirect. In that case, the customer will NOT return to the TERMURL since they ended the process. In this case, you will NOT call /ThreeDSaleTransactions.

**If merchant is doing Authorizations, the endpoint would be /ThreeDAuthorizeTransactions.

Step 7 The merchant parses the JSON response and sends the cardholder payment confirmation.

VERIFY ENROLLMENT TRANSACTIONS

OPERATION END-POINT

The URL to submit verify enrollment transactions is as follows:
https://api.ugpayments.ch/merchants/<merchantid>/checkenrollment

VERIFY ENROLLMENT TRANSACTION REQUEST

The following table lists the elements for verify enrollment transactions:

Parameter Name	Description	Example
siteId	Site ID assigned by Unicorn Integer, mandatory	12
amount	Amount of the transaction Decimal, mandatory	123.45
currency	Transaction currency, in ISO 4217 format. 3 character, mandatory	USD
firstName	Cardholder's first name 50 character max, mandatory	John
lastName	Cardholder's last name 50 character max, mandatory	Doe
phone	Cardholder's phone 20 character max, mandatory	555-555-5555
addressLine1	Billing address 100 character max, mandatory	123 Fake St.
addressLine2	Billing address 100 character max, optional	Suite # 789
city	Billing address city 50 character max, mandatory	Hollywood
state	Billing state	California

	50 character max, mandatory	
countryId	Billing country 2 character, mandatory	US
postalCode	Billing postal code 20 character max, mandatory	90046
email	Cardholder's email address 100 character max, mandatory	<identifier>@<domain>.<extension>
cardNumber	Credit card number 50 character max, mandatory	4024007118676898
nameOnCard	Cardholder's name printed on card 40 character max, mandatory	John J. Doe
expirationMonth	2 character, mandatory	09
expirationYear	4 character, mandatory	2018
cVVCode	4 character max, mandatory	469
iPAddress	Cardholder's IP Address 20 character max, mandatory	127.0.0.1
trackingId	Merchant Provided number, example reference number or merchant's transactionID 100 character max, optional	123456
isInitialForRecurring	Indicates if the transaction is the initial recurring transaction, if recurring, send true, mandatory	true or false *PLEASE NOTE, IF SET TO TRUE THEN 3D WILL ALLOWS RESPOND WITH CHALLENGE REQUEST. IF SET TO FALSE, YOU MAY GET A FRICTIONLESS RESPONSE BACK.
ConfirmURL	Merchant's URL that can receive a postback/callback	https://www.merchanturl.com/postback.php

BrowserData [array]		
ScreenHeight	Total Height of cardholder's screen in pixels 6 character max, mandatory	1080
ScreenWidth	Total Width of cardholder's screen in pixels 6 character max, mandatory	1920
ColorDepth	Value representing the bit depth of the color palette for displaying images in bits per pixel 2 character max, mandatory	1, 4, 8, 15, 16, 24, 32, 48 **Please note, if color depth is outside of above numbers, submit the closest. Example if color returned is 30, submit 32.**
IsJavaEnabled	The ability of the cardholder browser to execute Java. Boolean, mandatory	true, false
IsJavaScriptEnabled	The ability of the cardholder browser to execute JavaScript. Boolean, mandatory	true, false
TimeZone	Time-zone offset in minutes between UTC and the cardholder browser local time. 5 characters, mandatory	-300
AcceptHeaders	Exact content of the HTTP accept headers as sent to the 3DS Requestor from the cardholder's browser. 2048 character max, mandatory	text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image……

AcceptLanguage	Value representing the browser language as defined in IETF BCP47. 8 character max, mandatory	en-US
UserAgent	Exact content of the HTTP user-agent header. 2048 character max, mandatory	Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36……

JSON Format Example:

{"siteId":"11",
"amount":123.45,
"currency":"USD",
"firstName":"John",
"lastName":"Doe",
"phone":"555-555-5555",
"addressLine1":"123 Fake St.",
"addressLine2":"",
"city":"Hollywood",
"state":"CA",
"countryId":"US",
"postalCode":"12345",
"email":"",
"cardNumber":4024007118676898,
"nameOnCard":"John J Doe",
"expirationMonth":11,
"expirationYear":2019,
"cVVCode":"402",
"iPAddress":"127.0.0.0",
"trackingID" : "123",
"isInitialForRecurring":false,
"ConfirmURL": https://www.merchanturl.com/post.php,
"browserdata": {
"AcceptHeaders":
"text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7",
"UserAgent": "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/120.0.0.0 Safari/537.36",
"AcceptLanguage": "en-US",
"ColorDepth": "8",
"IsJavaEnabled": true,
"IsJavaScriptEnabled": true,
"ScreenHeight": "480",
"ScreenWidth": "640",
"TimeZone": "-300"

}
}

CHECK ENROLLMENT TRANSACTION RESPONSE

The result is in JSON format with the following elements:

Parameter Name	Description	Example
state	The type of transaction	Verify
status	The transaction status	Successful
message	The bank message	Card Enrolled, initialized
description	Any additional message with the transacton	Challenge Required; Additional authentication is required using the CReq/CRes.
Result Array		
EnrollmentStatus	The card holders enrollment status Y – Enrolled F – Challenge/fingerprint	Y, F
AcsUrl	Enrollment server URL.	https://www.visa.com/someacsurl
AuthType	The authentication type	doFingerPrinting, doChallenge
End Array		
trackingId	Merchant's internal transactionID (optional)	123343
postbackURL	Postbackurl from Unicorn	This can be ignored.
version	Version of 3D integration	StreamLine
id	The id of the verify id from the /checkenrollment transaction	123456 – **this has to be passed to the AcsUrl**

EXAMPLE REQUESTS

Example 1: Status = /checkenrollment declined, cardholder not enrolled (scenario card for testing: 4012001037141112, Any Name on Card, Amount = 150.00, Any valid Expiry EX: 12/2028, CVV 196)

{
  "state": "Verify",
  "status": "Declined",
  "message": "User Authentication Failed",
  "reasonCode": "C1 - Declined",

"result":   [
 { },
  ],
"trackingId": 1234 - internal merchant transaction id - optional
  "postbackURL": https://quickpay.ugpayments.ch/verify - this can be ignored
  "version": StreamLine
  "id": "26357791"
}

In this scenario, 3D verify/authentication is NOT successful, so no 3D Sale can be processed. This ends the sale attempt.

Example 2: Status = /checkenrollment successful, cardholder enrolled, frictionless response (scenario card for testing: 4200000000000026, Any Name on Card, Amount = 150.00, Any valid Expiry EX: 12/2028, CVV 196)

{
  "state": "Verify",
  "status": "Successful",
  "message": "Authentication successful (frictionless flow)",
  "description": "No challenge required, frictionless authentication successful. Please proceed for 3D sale.",
   "reasonCode": "00 - Approved",

"result":   [
 {
      "responseKey": "EnrollmentStatus",
      "responseValue": "Y"
    },
  ],
"trackingId": 1234 - internal merchant transaction id - optional
  "postbackURL": https://quickpay.ugpayments.ch/verify - this can be ignored
  "version": StreamLine
  "id": "26357791"
}

The merchant can then call the /ThreeDSaleTransactions endpoint by passing the VerifyTransactionId (if recurring is needed, also pass the field IsInitialForRecurring = true) with the value of id returned in the response from the previous request to /checkenrollment and the liability shift is away from the merchant.

At this point, the merchant will get a response from the sale attempt:

Success:

{
  "state": "Sale",
  "status": "Successful",
  "message": " The test operation was successfully processed.",
  "id": "181763"
}

Example 3: Status = /checkenrollment successful, cardholder enrolled, acsChallenge response, challenge required, (scenario card for testing: 4200000000000042, Any Name on Card, Amount = 150.00, Any valid Expiry EX: 12/2028, CVV 196, OTP 123456)

{
  "state": "Verify",
  "status": "Successful",
  "message": "transaction pending",
  "description": "Browser Figerprinting Required. Authentication is required to collect the client's browser data required for the 3DS.",
  "reasonCode": "1000 - Unknown",

"result":   [
 {
       "responseKey": "EnrollmentStatus",
       "responseValue": "F"
        "responseKey": "AcsUrl",
       "responseValue": "https://quickpay.ugpayments.ch/acsfingerprinting"
       "responseKey": "AuthType",
       "responseValue": "doFingerPrinting"

     },
  ],
"trackingId": 1234 - internal merchant transaction id - optional
  "postbackURL": https://quickpay.ugpayments.ch/verify - this can be ignored
  "version": StreamLine
  "id": "26357791" – **this is the verify transactionID you will send to /ThreeDSaleTransactions**
}

The Merchant will then redirect the customer to the AcsUrl using an HTML Form post with the following parameters:

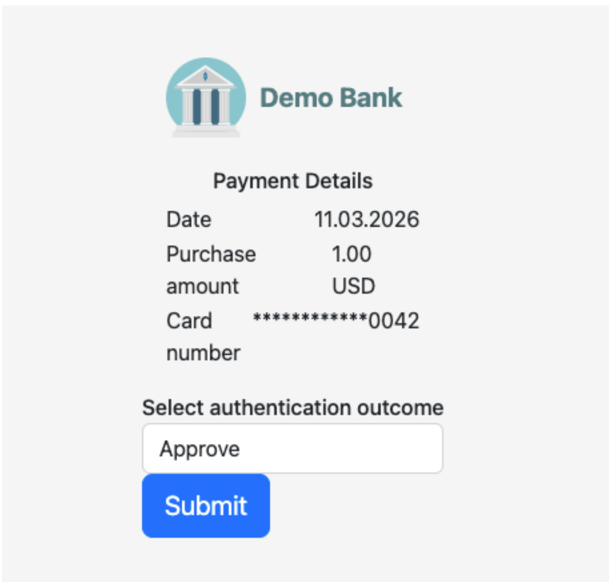
Field Name	Value
AcsUrl	The authenticationURL returned by the card issuer for authentication

TermUrl	The merchant’s page that will collect the authentication response and process the sale
transactionId	The VerifyTransactionId
AuthType	The AuthType returned from the /checkenrollment request

Example HTML FORM:

```
<form name="acs" method="post" action="https://quickpay.ugpayments.ch/acsfingerprinting">
   <input name="transactionId" type="hidden" value="26357791" /><br />
   <input name="AuthType" type="hidden" value="doFingerPrinting" />
   <input name="TermUrl" type="hidden" value="http://merchantssite.com/process3dsale.php" />
   <input type="submit" value="Authenticate ACS URL" />
</form>
```

The customer will then get to their bank’s ACS/OTP/Authentication Page. In this example, you can select the authentication outcome.



The Merchant will get the following as POST values to the TermUrl:

```
{
  "Status": "Successful",
  "State": "Verify",
  "Message": "Two-step transaction succeeded”,
  "Id": "26359398",
  "TrackingId": "123456",
}
```

The merchant can then call the /ThreeDSaleTransactions endpoint by passing the VerifyTransactionId (if recurring is needed, also pass the field IsInitialForRecurring = true) with the value of id returned in the response from the previous request to /checkenrollment and the liability shift is away from the merchant.

At this point, the merchant will get a response from the sale attempt:

Success:

```
{
  "state": "Sale",
  "status": "Successful",
  "message": "  The test operation was successfully processed.",
  "id": "181763"
}
```

Example 4: Status = /checkenrollment successful, cardholder enrolled, acsChallenge response, challenge required failed, (scenario card for testing: 4200000000000042, Any Name on Card, Amount = 150.00, Any valid Expiry EX: 12/2028, CVV 196, OTP 123456789)

```
{
  "state": "Verify",
  "status": "Successful",
  "message": "transaction pending",
  "description": "Browser Figerprinting Required. Authentication is required to collect the client's browser data required for the 3DS.",
  "reasonCode": "1000 - Unknown",

"result":   [
 {
       "responseKey": "EnrollmentStatus",
       "responseValue": "F"
        "responseKey": "AcsUrl",
       "responseValue": "https://quickpay.ugpayments.ch/acsfingerprinting"
       "responseKey": "AuthType",
       "responseValue": "doFingerPrinting"


    },
  ],
"trackingId": 1234 - internal merchant transaction id - optional
  "postbackURL": https://quickpay.ugpayments.ch/verify - this can be ignored
  "version": StreamLine
  "id": "26357791" – this is the verify transactionID you will send to /ThreeDSaleTransactions
}
```

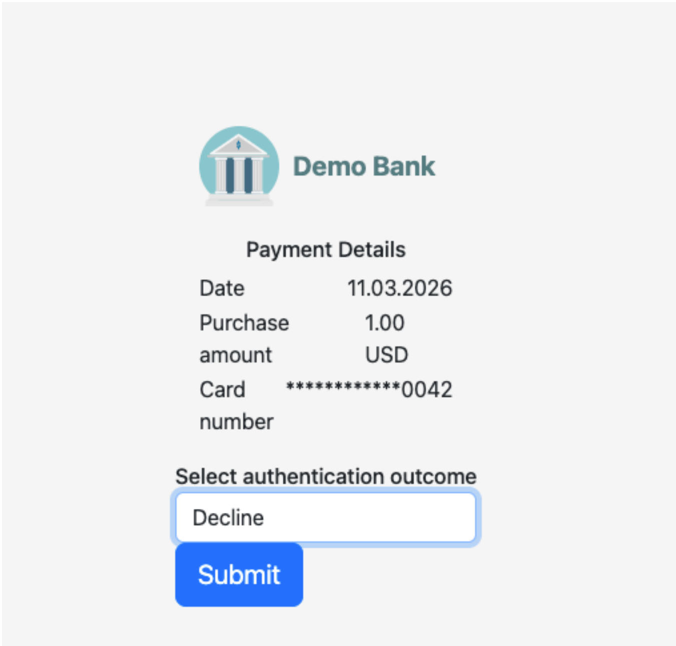
The Merchant will then redirect the customer to the AcsUrl using an HTML Form post with the following parameters:

Field Name	Value
AcsUrl	The authenticationURL returned by the card issuer for authentication
TermUrl	The merchant’s page that will collect the authentication response and process the sale
transactionId	The VerifyTransactionId
AuthType	The AuthType returned from the /checkenrollment request

Example HTML FORM:

```html
<form name="acs" method="post" action="https://quickpay.ugpayments.ch/acsfingerprinting">
   <input name="transactionId" type="hidden" value="26357791" /><br />
   <input name="AuthType" type="hidden" value="doFingerPrinting" />
   <input name="TermUrl" type="hidden" value="http://merchantssite.com/process3dsale.php" />
   <input type="submit" value="Authenticate ACS URL" />
</form>
```

The customer will then get to their bank’s ACS/OTP/Authentication Page. In this example, you can select Decline



The Merchant will get the following as POST values to the TermUrl:


```
{
  "Status": "Declined",
  "State": "Verify",
  "Message": "User Authentication Failed.”,
  "Id": "26359398",
  "TrackingId": "123456",
}
```


In this scenario, 3D verify/authentication is NOT successful, so no 3D Sale can be processed. This ends the sale attempt.

THREEDSALE TRANSACTION REQUEST

The following table lists the elements for threedsale:

Parameter Name	Description	Example
VerifyTransactionId	Transaction id returned from the /checkenrollment in the value of id	122100
ConfirmURL	A URL on merchant's server that will listen for a postback or callback	https://www.somesite.com/postback.php

Success:


```
{
  "state": "Sale",
  "status": "Successful",
  "message": " Request successfully processed in 'Merchant in Connector Test Mode",
  "description": " Approved",
  "reasonCode": " 00 - Approved",
  "id": "181763"
}
```


To Rebill this transaction, always use the id returned on the sale.

Decline:


```
{
  "state": "Sale",
  "status": "Declined",
  "message": " Decline",
  "id": "181763"
}
```


ACS POST FORM

The AcsUrl is where the customer may be asked to authenticate by a OTP. This url is often times on either the issuers site or a generic OTP provider.

Example Form:

```
<form name="acs" method="post" action="<acsurl_value> ">
   <input name="transactionId" type="hidden" value="3605449" /><br />
   <input name="AuthType" type="hidden" value="doChallenge" />
   <input name="TermUrl" type="hidden" value="http://merchantssite.com/process3dsale.php" />
   <input type="submit" value="Authenticate ACS URL" />
</form>
```

At this point, the cardholder will be presented with the authentication challenge. The cardholder will be redirected back to the merchant's "TermURL" passed in the acs redirection with the following values in an HTTP POST:

If challenge was failed, or cardholder canceled, the post response will be as follows:


```
{
  "Id": "300003",
  "TrackingId": "Merchant123",
  "Amount": " 10.00 ",
  "Message": " authenticated ",
  "State": " Verify ",
  "Status": "Declined"
}
```


If challenge was successfully authorized, the response will be as follows:


```
{
  "Id": "300003",
  "TrackingId": "Merchant123",
  "Amount": " 10.00 ",
  "Message": " authenticated ",
  "State": " Verify ",
  "Status": "Successful"
}
```


The merchant can call the /ThreeDSaleTransactions endpoint by passing the VerifyTransactionId (if recurring is needed, also pass the field IsInitialForRecurring = true) with the value of Id returned in the post response to the merchant's termurl and the liability shift is away from the merchant.

At this point, you will get a response from the sale attempt.

Success:


```
{
  "state": "Sale",
  "status": "Successful",
  "message": " authorized",
  "resonCode": " 00 - Approved",
  "result":    [
         {
      "responseKey": "LiabilityShiftIndicator",
      "responseValue": "Y"
    },
  ],
  "id": "181763"
}
```


To Rebill this transaction, always use the id returned on the sale.

Decline:


```
{
  "state": "Sale",
  "status": "Declined",
  "message": " Decline",
  "id": "181763"
}
```


TRANSACTION STATUS RESPONSES

3-D Secure2.0 Version: 3.1

Success
A successful verify transaction indicates that the cardholder is 3D Secure enrolled.

Declined
A declined transaction indicates that the cardholder is not enrolled, enrollment could not be determined or there was an error. The Response message will provide additional information.

Error
An internal system error occurred.

ENROLLMENT STATUS RESPONSES

If the verify enrollment transaction is successful or declined an enrollment status code will be returned in the Result field.

The following table shows the meaning of the enrollment status code.

Condition	Status	Description
Card/Cardholder enrolled	Y	Enrollment successful: The card is enrolled in the 3-D Secure program and eligible for 3-D authentication.
Challenge/Fingerprinting	F	Enrollment successful: The card is enrolled, and a challenge or fingerprinting is requested.

CARD/CARDHOLDER ENROLLED (Y) OR (F)

The Acsurl will be returned in the result.

Step 1:

The merchant sends an HTTP post to ACSUrl with the following variables:

Field Name	Value
AcsUrl	The authenticationURL returned by the card issuer for authentication
TermUrl	The merchant's page that will collect the authentication response and process the sale
transactionId	The VerifyTransactionId
AuthType	The AuthType returned from the /checkenrollment request

Example:

```
<form name="acs" method="post" action="<acsurl_value> ">
   <input name="transactionId" type="hidden" value="3605449" /><br />
   <input name="TermUrl" type="hidden" value="http://merchantssite.com/process3dsale.php" />
   <input name="AuthType" type="hidden" value="doChallenge" />
   <input type="submit" value="Authenticate ACS URL" />
</form>
```

Step 2:
After the customer authenticates from the bank's ACS, the ACS redirects the cardholder back to the merchant's TermUrl.

If successful, the customer will return to the Merchant's Termurl with the an HTTP POST with the following variables:

"Id": "300003",
"TrackingId": "Merchant123",
"Amount": " 10.00 ",
"Message": " authenticated ",
"State": " Verify ",
"Status": "Successful"

The merchant then will submit the verify transaction id to the /threedsaletransactions endpoint. (If recurring is needed, please pass 'IsInitialForRecurring' => 'true',)

CARD/CARDHOLDER NOT ENROLLED(N)

Response will be "card not enrolled"

SYSTEM ERROR(E)

An enrollment check could not be completed. The transaction is ineligible for 3-D secure processing.

3-D SALE/AUTHORIZE TRANSACTION

REQUIREMENTS:

1. The Enrollment status must be Card/Cardholder enrolled(Y) or (F)

OPERATION END-POINT

The URL to submit 3D Sale transactions is as follows:
https://api.ugpayments.ch/merchants/<merchantid>/ThreeDSaleTransactions

The URL to submit 3D Authorize transactions is as follows:
https://api.ugpayments.ch/merchants/<merchantid>/ThreeDAuthorizeTransactions

3D SALE/AUTHORIZE TRANSACTION REQUEST

The following table lists the elements for 3D Sale and Authorize transactions:

Parameter Name	**Description**	**Example**
VerifyTransactionID	The identifier of the verify enrollment transaction	123456

JSON Format Example:
{"VerifyTransactionId":"171755",
}

3D SALE/AUTHORIZE TRANSACTION RESPONSE

The result is in JSON format with the following elements:

Parameter Name	Description	Example
Id	The id of the verify enrollment transaction	171888
Message		
State	The type of transaction. Please refer to Appendix A for detail.	Sale
Status	The transaction status. Please refer to Appendix B for detail.	Successful

Example Response JSON:
{
"state": "Sale",
"status": "Successful",
"message": "",
"id": “171888"
}

CAPTURE TRANSACTIONS

URL: https://api.ugpayments.ch/merchants/[MerchantId]/capturetransactions
Only authorize transactions that have not been voided can be captured. You will use the /ThreeDAuthorize transaction id.

JSON REQUEST PARAMETERS

Parameter Name	**Description**	**Example**
authorizetransactionid	The transaction id return by the Authorization String, mandatory	123456
amount	Amount of the transaction Decimal/Number, mandatory	123.45

JSON RESPONSE PARAMETERS

Parameter Name	Description	Example
State	String, state of transaction, example Sale, Auth, Refund	Sale
Status	String, Status of transaction	Approved
message	String, message regarding the transaction	The operation was successfully processed.
trackingId	String, passed from request	YourID
id	String, transactionID from UnicornGroup	transactionID
reasonCode	String, Response From bank ONLY if transaction reached bank.	00 - Approved

HTTP REQUEST EXAMPLE


```
{
        "authorizeTransactionId": "123456",
        "amount": 123.45
}
```


HTTP RESPONSE EXAMPLE


```
{
        "id": "123456",
        "message": "Success",
        "state": "Capture",
        "status": "Successful"
        "reasoncode": "00-approved"

}
```


VOID TRANSACTIONS

URL: https://api.ugpayments.ch/merchants/[MerchantId]/voidtransactions
Only authorize transaction can be voided.

JSON REQUEST PARAMETERS

Parameter Name	Description	Example
authorizeTransactionid	The transaction id returned by the authorization. String, mandatory	123456

JSON RESPONSE PARAMETERS

Parameter Name	Description	Example
State	String, state of transaction, example Sale, Auth, Refund	Sale
Status	String, Status of transaction	Approved

message	String, message regarding the transaction	The operation was successfully processed.
trackingId	String, passed from request	YourID
id	String, transactionID from UnicornGroup	transactionID
reasonCode	String, Response From bank ONLY if transaction reached bank.	00 - Approved

HTTP REQUEST EXAMPLE


```
{
	"authorizeTransactionId": "123456"
}
```


HTTP RESPONSE EXAMPLE


```
{
	"id": "123457",
	"message": "Success",
	"state": "Void",
	"status": "Successful"
	"reasoncode": "00-approved"

}
```

3-D SALE REBILL

If you wish to rebill a previously authenticated transaction, you can use the /recurringtransactions endpoint. You must use the Sale Transaction ID returned from the /ThreeDSaleTransactions endpoint.

URL: https://api.ugpayments.ch/merchants/[MerchantId]/recurringtransactions
Only sale transactions can be rebilled.

If you wish to rebill any transaction, you must send 'IsInitialForRecurring' = 'true' on every endpoint on the 3D flow:

/checkenrollment
/threedsaletransactions

3D SALE REBILL REQUEST

The following table lists the elements for rebilling 3D transactions:

Parameter Name	**Description**	**Example**
referenceTransactionID	The identifier of the sale transaction	123456
Amount	The amount of the transaction you wish to charge again	2.45

3D SALE REBILL RESPONSE

The result is in JSON format with the following elements:

Parameter Name	Description	Example
Id	The id of the rebilled transaction	171888
Message	Message from bank response	APPROVED
State	The type of transaction. Please refer to Appendix A for detail.	Recurring
Status	The transaction status. Please refer to Appendix B for detail.	Successful

HTTP REQUEST EXAMPLE

```
{
	"referenceTransactionId": "123456",
	"amount": 123.45
}
```

HTTP RESPONSE EXAMPLE


```
{
	"id": "123456",
	"message": "Success",
	"state": "Recurring",
	"status": "Successful"
	"reasoncode": "00-approved"

}
```


CONFIRM PAGE

When a customer has successfully completed a transaction, UnicornGroup will send an HTTP POST with the transaction details back to a designated page on your site. This page should validate and store the transaction information in your database. The confirm page provides communication between UnicornGroup and your application and does not need to provide user functionality.
Information is posted to the confirm page as standard HTTP POST name-value pairs (NVP) separated by ampersands (&). An example confirm post would be:
Amount=17.99&MerchantReference=abc123&PayReferenceID=b9ab260b-d690-4507-8d56-8bd92c4c132a&TransactionID=4cfdefc3-6ad2-49de-a25b-5d0f41e8cd1a

The following fields are transmitted by UnicornPayment in a transaction to the ConfirmURL specified by you:

[TrackingId] => Reference Number for the Merchant's Records (Limit 100 characters
[MerchantReference] => Reference Number for the Merchant's Records (Limit 100 characters)
[CurrencyID] => ISO Currency Code
[Key] => key supplied from portal from UnicornPayment
[Amount] => Amount of Transaction (Money/Numeric/Decimal)
[TransactionID] => Identity Number for the Transaction (Numeric)
[CardMask] => Characters used to mask the card number
[TransactionState] => State of Transaction (Appendix A)
[TransactionStatus] => State of Transaction (Appendix B)
[ShippingFirstName] => First Name for Shipping Address (Limit 50 characters)
[ShippingLastName] => Last Name for Shipping Address (Limit 50 characters)
[ShippingAddress1] => Address Line 1 for Shipping Address (Limit 100 characters)
[ShippingAddress2] => Address Line 2 for Shipping Address (Limit 100 characters)
[ShippingCity] => City for Shipping Address (Limit 50 characters)
[ShippingState] => State for Shipping Address (Limit 50 characters)
[ShippingCountry] => Country for Shipping Address
[ShippingPostalCode] => Postal Code for Shipping Address (Limit 20 characters)
[CustomerEmail] => mailto:mail@mail.com Email for the Customer (Limit 50 characters)
[CustomerFirstName] => First Name of Customer (Limit 50 characters)
[CustomerLastName] => Last name of Customer (Limit 50 characters)
[CustomerAddress1] => Address Line 1 for Customer Address (Limit 100 characters)
[CustomerAddress2] => Address Line 2 for Customer Address (Limit 100 characters)

[CustomerCity] => City for Customer Address (Limit 50 characters)
[CustomerState] => State for Customer Address (Limit 50 characters)
[CustomerCountry] => Country for Customer Address
[CustomerPostalCode] => Postal Code for Customer Address (Limit 20 characters)
[CustomerPhone] => Customer's Phone (Limit 20 characters)
[SiteID] => Site Id for the Merchant's Site (Numeric)

REFUND TRANSACTIONS

REFUND TRANSACTIONS

URL: https://api.ugpayments.ch/merchants/[MerchantId]/refundtransactions
Only sale and capture transactions can be refunded.

JSON REQUEST PARAMETERS

Parameter Name	Description	Example
referencetransactionid	The transaction id returned by the sale transaction or the capture transaction. String, mandatory	123456
amount	The amount to refund, not to exceed original transaction amount. Decimal/Number, mandatory	123.45

JSON RESPONSE PARAMETERS

Parameter Name	Description	Example
State	String, state of transaction, example Sale, Auth, Refund	Sale
Status	String, Status of transaction	Approved
message	String, message regarding the transaction	The operation was successfully processed.
trackingId	String, passed from request	YourID
id	String, transactionID from UnicornGroup	transactionID
reasonCode	String, Response From bank ONLY if transaction reached bank.	00 - Approved

HTTP REQUEST EXAMPLE

```
{
	"referenceTransactionId": "123456",
```

```
	"amount": 123.45
}
```

HTTP RESPONSE EXAMPLE

```
{
	"id": "123456",
	"message": "Success",
	"state": "Refund",
	"status": "Successful"
	"reasoncode": "00-approved"

}
```

APPENDIX A – TRANSACTION STATE TYPES

Sale
Authorize
Capture
Void
Refund

APPENDIX B – TRANSACTION STATUS TYPES

Successful
Error
Declined
Pending
Scrubbed
Fraud
Unconfirmed

APPENDIX C – VALIDATION ERRORS

ACS Verification Id is required when supplying ECI or XID.

Address Line1' can not contain a credit card number.
Address Line1' must be between 0 and 100 characters. You entered <char> characters.
Address Line1' must be between 1 and 100 characters.
Address Line2' can not contain a credit card number.
Address Line2' must be between 0 and 100 characters. You entered <char> characters.
Address Line2' must be between 1 and 100 characters.
Amount' must be greater than '0'.
Authorize Transaction Id' is not valid.
Bank Identifier' should not be empty.
Card Number' is not valid.
City' can not contain a credit card number.
City' must be between 0 and 50 characters. You entered <char> characters.
City' must be between 1 and 50 characters
Country Id' is not valid.
Country Id' must be not be empty.
'Currency' can not contain a credit card number.
Currency' is not valid.
'CVV code' is not valid.
ECI is required when supplying ACS Verification Id or XID.
Email'   must be between 0 and 100 characters. You entered <char> characters.
Email'   must be between 1 and 100 characters. You entered <char> characters.
Email'   should not be empty.
Email' can not contain a credit card number.
Expiration date' is not valid.
First Name' can not contain a credit card number.
First Name' must be between 1 and 50 characters. You entered <char> characters.
First Name' should not be empty.
IP Address' can not contain a credit card number.
IP Address' must be between 0 and 20 characters. You entered <char> characters.
Last Name' can not contain a credit card number.
Last Name' must be between 1 and 50 characters. You entered <char> characters.

Last Name' should not be empty.
Merchant Referrer Url' must be between 0 and 100 characters. You entered <char> characters.
Name On Card' can not contain a credit card number.
Phone' must be between 0 and 20 characters. You entered <char> characters.
Phone' must be between 1 and 20 characters. You entered <char> characters.
Phone' should not be empty.
Postal Code' must be between 0 and 20 characters. You entered <char> characters.
Postal Code' must be between 1 and 20 characters in length.
Reason Id' is not valid.
Reference Transaction Id' is not valid.
Return Url' should not be empty.
'Sale Transaction Id' is not valid.
Shipping Address Line1' can not contain a credit card number.
Shipping Address Line1' must be between 0 and 100 characters. You entered <char> characters.
Shipping Address Line2' can not contain a credit card number.
Shipping Address Line2' must be between 0 and 100 characters. You entered <char> characters.
Shipping City' can not contain a credit card number.
Shipping City' must be between 0 and 50 characters. You entered <char> characters.
Shipping Country Id' can not contain a credit card number.
Shipping Country Id' is not valid.
Shipping First Name' can not contain a credit card number.
Shipping First Name' must be between 0 and 50 characters. You entered <char> characters.
Shipping Last Name' can not contain a credit card number.
Shipping Last Name' must be between 0 and 50 characters. You entered <char> characters.
Shipping Phone' must be between 0 and 20 characters. You entered <char> characters.
Shipping Postal Code' can not contain a credit card number.
Shipping Postal Code' must be between 0 and 20 characters. You entered <char> characters.
Shipping State' can not contain a credit card number.
Shipping State' must be between 0 and 50 characters. You entered <char> characters.
Site Id' can not contain a credit card number.
'Site Id' is not valid.

'State' can not contain a credit card number.
State' must be between 0 and 50 characters. You entered <char> characters.
State' must be between 1 and 50 characters.
Subscription plan id' is not valid.
Token Id' is not valid.
Tracking Id' must be between 0 and 100 characters. You entered <char> characters.
Validation error for input parameters.
Verify Transaction Id' is not valid.
XID is required when supplying ECI or ACS Verification Id.

APPENDIX D – SCRUB MESSAGES

Amount Limit
Approved Refferer Url Required
Card Bank ID Number IP Address
Card Decline Limiting
Card Holder Name
Card Limit
Country Black List
Credit Card Name and Customer Name Match
CVV2 Required
CyberSource
Email Limit
Email Required
Expired Credit Card
IP Address Bill
IP Black List
Name Credit Card Match
Name Declined Limit
Name Limit
Non US Customer
Phone Required
Price Limit

Price Minimum/Maximum
Refund Limit
Region Black List

APPENDIX E – ERROR MESSAGE

3D security is not enabled for this merchant.
Account associated with token is either deleted or disabled.
An address is required for this transaction.
An internal exception has occurred. Please refer to Error Id - <errorid>
Authorization headers not contained in the request.
Cannot do a full charge back for this transaction. Only partial charge back is allowed.
Cannot do a full refund for this transaction. Only partial refund is allowed.
Cannot do a full retrieval for this transaction. Only partial retrieval is allowed.
Capture amount is greater than the remaining authorization amount to be captured.
Capture is not enabled.
Cascade set up not valid for this transaction.
Client is not valid.
Credit card token used for transaction is no longer valid.
Critical error. Contact Unicorn.
Direct integration is not enabled.
Forced capture must have a bank reference as well.
Forced refund must have a bank reference as well.
Invalid Permissions.
Invalid principal identity.
Invalid transaction parameter(s).
Merchant does not exist or is no longer active.
Not a valid user.
Not able to capture. The transaction might be voided or already captured.
Not able to refund. The transaction might have CBK1 record or is already refunded.
Not authorized to access this resource.

Not authorized to execute this method.
Null Reason Code or specified Reason Code does not match the Card and Transaction Type thus cannot be authorized.
Partial charge back amount is greater than the remaining amount to be charged back.
Partial refund amount is greater than the remaining amount to be refunded.
Partial retrieval amount is greater than the remaining amount to be retrieved.
Rates not available for credit card and currency type.
Refund is not enabled.
Request is not in correct format.
Service connection failed.
Site does not belong to the merchant.
Site does not exist or is no longer active.
Subscription plan is not valid.
Test card is not enabled.
The authenticaiton token in no longed valid.
The credit card number is blacklisted.
The site is missing required bank parameter.
The specified transaction is not valid for Blacklisting.
The specified transaction is not valid for CBK1 Credit.
The specified transaction is not valid for Charge back.
The specified transaction is not valid for Dispute.
The specified transaction is not valid for Void.
The specified transaction is not valid for Whitelisting.
The volume limit for transactions have been exceeded.
This account is currently disabled, please contact risk@UnicornGroup.com with any questions.
This function is not supported by the bank.
This transaction has already been captured.
This transaction is already been charged back.
This transaction is already been initiated for retrieval.
This transaction is already been refunded.
This transaction is already been voided.

Time period to capture this transaction has expired.
Transaction id is not valid.
Transaction is declined for failed 3D authentication. 3D authentication is required for this merchant.
Unable to locate successful transaction details.
User is disabled or is no longer active.
User not mapped to any account.
Virtual terminal is not enabled.

APPENDIX F – DECLINE MESSAGES

Code	Description	Category	Retry
0	Approved	Approved	n/a
83	Address verification completed; no authorisation was requested	Approved	n/a
5	Declined by the issuing bank; no reason supplied	Issuer decline	No - do not retry the same card
101	Authorisation declined by the issuing bank	Issuer decline	No - do not retry the same card
49	Transaction not permitted	Issuer decline	No - do not retry the same card
59	Issuer flagged the transaction as suspected fraud	Issuer decline	No - do not retry the same card
62	Card is restricted for this transaction type or region	Issuer decline	No - do not retry the same card

34	Transaction flagged as suspicious by the issuer	Issuer decline	No - do not retry the same card
57	Transaction type not permitted for this cardholder	Issuer decline	No - do not retry the same card
4	Card flagged for retention by the issuer	Issuer decline	No - do not retry the same card
41	Card reported lost	Issuer decline	No - do not retry the same card
43	Card reported stolen	Issuer decline	No - do not retry the same card
42	Card flagged for retention by the issuer	Issuer decline	No - do not retry the same card
12	Issuer rejected the transaction as invalid	Issuer decline	No - do not retry the same card
31	Issuer not accepted for this transaction	Issuer decline	No - do not retry the same card
58	Transaction not permitted for this acceptor	Issuer decline	No - do not retry the same card
3	Merchant configuration not recognised by the acquirer	Issuer decline	No - do not retry the same card
123	Blocked by the processor	Issuer decline	No - do not retry the same card
89	Declined for a security violation	Issuer decline	No - do not retry the same card

82	Security code (CVV/CVC) did not match	Data error	Yes - after correcting the data
14	Card number is not valid	Data error	Yes - after correcting the data
54	Card has expired	Data error	Yes - after correcting the data
92	Card type not supported for this account	Data error	Yes - after correcting the data
35	Account is not valid	Data error	Yes - after correcting the data
16	Expiry date is not valid	Data error	Yes - after correcting the data
30	Request was malformed	Data error	Yes - after correcting the data
13	Amount is not valid for this transaction	Data error	Yes - after correcting the data
93	Security code is required	Data error	Yes - after correcting the data
55	PIN was incorrect	Data error	Yes - after correcting the data
76	Account not found	Data error	Yes - after correcting the data
94	Currency not supported	Data error	Yes - after correcting the data
51	Insufficient funds	Limit	Yes - later, or with a lower amount
61	Amount exceeds the cardholder's limit	Limit	Yes - later, or with a lower amount
65	Transaction frequency limit exceeded	Limit	Yes - later, or with a lower amount
75	PIN retry limit exceeded	Limit	Yes - later, or with a lower amount
1	Cardholder must contact their issuing bank	Contact issuer	No - not without cardholder action

2	Cardholder must contact their issuing bank (special conditions)	Contact issuer	No - not without cardholder action
25	Issuer could not locate the account	Contact issuer	No - not without cardholder action
91	Issuing bank unavailable	Contact issuer	No - not without cardholder action
21	Issuer took no action	Contact issuer	No - not without cardholder action
26	Duplicate request; the previous record was replaced	Lifecycle	No - check the original transaction first
98	Reversal already processed	Lifecycle	No - check the original transaction first
107	Duplicate transaction	Lifecycle	No - check the original transaction first
19	Resubmit the transaction	Lifecycle	No - check the original transaction first
24	Cardholder revoked all authorisations	Lifecycle	No - check the original transaction first
23	Cardholder revoked authorisation for this order	Lifecycle	No - check the original transaction first
744	Cardholder stopped recurring payments	Lifecycle	No - check the original transaction first
114	Cardholder stopped the recurring payment	Lifecycle	No - check the original transaction first
22	Stop payment instruction received	Lifecycle	No - check the original transaction first

130	Security or configuration error	Technical	Yes - with backoff
A4	No response received in time	Technical	Yes - with backoff
124	Technical error at the acquirer	Technical	Yes - with backoff
99	Acquirer returned an error	Technical	Yes - with backoff
96	System error at the acquirer	Technical	Yes - with backoff
87	PIN key error	Technical	Yes - with backoff
8	Timed out	Technical	Yes - with backoff
6	Processing error	Technical	Yes - with backoff
63	Security key error at the acquirer	Technical	Yes - with backoff
118	Cryptographic failure	Technical	Yes - with backoff
81	PIN could not be verified	Technical	Yes - with backoff
1000	The acquirer did not supply a reason that could be mapped	Unspecified	No - treat as an issuer decline
C1	Declined; no specific reason supplied	Unspecified	No - treat as an issuer decline
11	Partially approved for a lower amount than requested	Approved	n/a
80	Approved for the purchase amount only; no cash back	Approved	n/a

7	Card flagged for retention by the issuer - suspected fraud	Issuer decline	No - do not retry the same card
39	No credit account is associated with this card	Issuer decline	No - do not retry the same card
52	No checking account is associated with this card	Issuer decline	No - do not retry the same card
53	No savings account is associated with this card	Issuer decline	No - do not retry the same card
77	Issuer does not participate in this service	Issuer decline	No - do not retry the same card
104	Transaction not allowed	Issuer decline	No - do not retry the same card
105	Transaction cannot be completed	Issuer decline	No - do not retry the same card
119	Declined for legal reasons	Issuer decline	No - do not retry the same card
15	Card issuer not recognised	Data error	Yes - after correcting the data
133	3-D Secure authentication failed; authenticate and retry	Data error	Yes - after correcting the data
137	Data error in the request	Data error	Yes - after correcting the data
131	Withdrawal limit exceeded	Limit	Yes - later, or with a lower amount
103	Authorisation requires	Contact issuer	No - not without cardholder action

	cardholder identification		
108	Card is blocked on first use; the cardholder must activate it	Contact issuer	No - not without cardholder action
84	Transaction is not valid at this point in its lifecycle	Lifecycle	No - check the original transaction first
79	Key validation error at the acquirer	Technical	Yes - with backoff
90	Acquirer cut-off in progress; retry shortly	Technical	Yes - with backoff
116	PIN could not be validated	Technical	Yes - with backoff
589	Transaction could not be routed	Technical	Yes - with backoff
602	System error; please try again	Technical	Yes - with backoff
200	Strong customer authentication required	Soft decline	Yes - retry with 3-D Secure authentication