ALLIED WALLET – DIRECT 3D

TABLE OF CONTENTS

REVISION HISTORY

Date	Revision	Description	Author
1/13/2015	1	First Version	Derek Baehr

OVERVIEW

WHAT IS 3-D SECURE

The Three Domain (3-D) Secure initiative by VISA is emerging to a new payment standard for secure handling of credit card transactions in electronic commerce. Communication between the three network domains is SSL-encrypted. Branded as Verified by Visa (VbV) and MasterCard SecureCode (MCSC), 3-D Secure is designed to clearly identify cardholders and accelerate the growth of electronic commerce through increased consumer confidence.

The authentication protocol uses Secure Sockets Layer (SSL) encryption to protect card information as it is transmitted across the Internet. Authentication is accomplished by verification of certain data which is maintained by the card issuing bank and identifies the individual making an online purchase as the legal owner of the card used.

3-D Secure is more than a payment authentication method or a technology definition. It is a model to isolate the liabilities of the various parties involved in the payment transaction cycle. The payment environment requires the participating cardholder to be registered (enrolled) for the process with his issuing bank. In essence, all parties involved in the payment flow must support the 3-D secure transactions. The 3-D framework requires the card issuing and acquiring banks to provide cardholders and merchants with an authentication methodology, without binding them to proprietary technology.

3-D SECURE PAYMENT AUTHENTICATION FLOW

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

Step 2 The merchant sends the payment details to the Allied Wallet hosted Verify Enrollment Transaction API

Step 3 Allied Wallet verifies if the merchant is 3-D Secure enabled and if the cardholder (the card itself) is 3-D-enrolled. If not, the merchant system proceeds with a standard transaction authorization request. If the cardholder is enrolled, the Allied Wallet system returns a Payment Authentication Request (PaReq) and Access Control Server URL (AcsUrl) to where the PAReq must be redirect by the merchant (Step 4).

Step 4 The merchant sends a HTTP POST request with the PAReq via the cardholder's browser to the issuing bank and includes the <TermUrl> and <MD>. The TermUrl (the web address of the merchant site) is required so that the issuer can later send the Payment Authentication Response (PARes) back to the merchant. The parameter type MD defines merchant-specific data. It can be left blank, but the element itself must be included in the PAReq.

Step 5 The cardholder's browser redirects the PAReq message to the issuer's (ACS) which authenticates the cardholder. This is done in two steps: First, the cardholder's browser sends an HTTPS request to the ACS. The server parses the data and invokes a login page in the cardholder's browser (popup or inline window).The cardholder now enters a password in the browser window and returns the data to the ACS.
Note: Many ACS servers automatically authenticate and redirect back to the TermUrl without requiring a password.

Step 6 Having received the data, the ACS authenticates the cardholder's password, constructs the

verification ID, and creates an SSL-encrypted and digitally signed Payer Authentication Response (PARes). Encryption and signature ensure that the cardholder cannot modify the content of the response message on its way to the merchant.

Step 7 The Payment Authentication Response (PARes) is posted by the ACS via the cardholder's browser to the merchant's web address TermUrl.

Step 8 The merchant system receives the PARes and forwards it to Allied Wallet ThreeDSaleTransactions or ThreeDAuthorizeTransactions API. With the authentication process completed, the Allied Wallet core system can now continue with the processing of the purchase order. This transaction request must contain the PARes obtained in Step 7 and the ID returned by the Verify Transaction.

Step 9 Allied Wallet responds to the merchant processing request with a ThreeDAuthorizeTransactions or ThreeDSaleTransactions response message.

Step 10 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:
http://<domain>/merchants/<merchantid>/verifytransaction

VERIFY ENROLLMENT TRANSACTION REQUEST

The following table lists the elements for verify enrollment transactions:

Parameter Name	Description	Example
siteId	Site ID assigned by Allied Wallet 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 50 character max, mandatory	California
countryId	Billing country 2 character, mandatory	US
postalCode	Billing postal code 20 bytes max, mandatory	90046
email	Cardholder's email address 100 character max, mandatory	<identifier>@<domain>.<extension>
cardNumber	Credit card number 50 character max, optional	4024007118676898
nameOnCard	Cardholder's name printed on card 40 bytes 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 100 character max, mandatory	123456
isInitialForRecurring	Indicates if the transaction is the initial recurring transaction	true or false

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 }

VERIFY ENROLLMENT TRANSACTION RESPONSE

The result is in JSON format with the following elements:

Parameter Name	Description	Example
id	The id of the verify enrollment transaction	123456
message	Error specific details	
result		
EnrollmentStatus	The card holders enrollment status Y – Enrolled N – Not Enrolled U – Ineligible E - Error	Y
AcsUrl	Enrollment server URL. Only returned if cardholder is enrolled	https://www.visa.com/someacsurl
PAReq	The Payer Authentication Request Only returned if cardholder is enrolled	
state	The type of transaction	Verify
status	The transaction status	Successful

Example 1: Status = Decline – cardholder not enrolled


```
{
  "state": "Verify",
  "status": "Successful",
  "message": "",
  "result": [  {
    "responseKey": "EnrollmentStatus",
    "responseValue": "N"
  }],
  "id": "181772"
}
```


Example 2: Status = Successful, cardholder enrolled


```
{
  "state": "Verify",
  "status": "Successful",
  "message": "",
  "result":   [
        {
      "responseKey": "EnrollmentStatus",
      "responseValue": "Y"
    },
        {
      "responseKey": "PAReq",
      "responseValue":
"eJxVUm1TwjAM/iu7fR9tx8aQy+oNQcUTQQX93HUBxu0FtyLgr7edQ7F3vcuTJk+SJ4XrY55Zn1jVaVmENutQ28JClklarEN7ubh1+rZVK1EkIisLDO0T1v
Y1h8WmQhy9otxXyGGKdS3WaKVJaO+EexUHsRdIh7kxdTwhhSPwqu8IRgMRd1dJ7K9sDvPoBT84tLW5Lt1xgZyh5qzkRhSKg5Afw8kT93o91/eBtBBy
rCYj7lPK/MDvMiA/DihEjjzKshQT611kGSrrUSVAGj/Icl+o6sT7bg/IGcC+yvhGqd2AkMPh0BFN9qFJ7sgyB2ICgPz1NN8bq9aExzThz18TNluM6XSr72Jyn
I0km26X/nQ0DoGYCEiEQu5S5jHdsOXSAesPvABI4weRm04488x8PzbsTIno4uHSAVr4Si9KD+JRPcgZAR53ek86Qmv5awP56/fm3igqlZYqipbr22E0vB
tu7sfpw9vNWEbtCY3OTZBhTLVGrMdYQ2kAEEND2hWSdv/a+vcvvgHaqMXj"
    },
        {
      "responseKey": "AcsUrl",
      "responseValue":
"https://aacsw.3ds.verifiedbyvisa.com/aacs/pahandler?vgtli=000520141001181847122255084700000000000;vgp=eNo1jrEOgjAYhHeeoukuBb
To8LcEghYWF8W9gYY0gVaBKLy9mOJtd98ld5DMfYfeahi1NQyHfoCRMrVttGkZru6X3QmjcZKmkZ01iuFFjTjhHjwE99AqkPUrK6%2F8EMcRpUA261i
vhjLnNAhCeqT7EIgLHNxG%2BbrpR0D%2B1sHnYOeFp2mVpWIq2mnRtzgXRfkRRCgdyzMD4joekN%2BXLwuwOiQ%3D.A32AEEAA"
    }
  ],
  "id": "181763"
}
```

TRANSACTION STATUS RERSPONSES

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.

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. A PaReq and AcsUrl are available.
Card/Cardholder not enrolled	N	Enrollment attempt accepted: The card is not enrolled in the 3-D Secure program, but is eligible for 3-D processing. It does not require authentication. The merchant proceeds with the purchase as an attempted authentication. He may exercise his right to dispute the transaction and claim a liability shift based on the ECI code. Should the cardholder later dispute the purchase; the Issuer may not submit a chargeback request.
Unable to verify enrollment	U	Enrollment failed: Visa or MasterCard were unable to verify if the cardholder is registered. The card cannot be enrolled for 3-D Secure and is therefore ineligible for 3-D processing.
A system error prevented enrollment from completion	E	Enrollment failed: The MPI system encountered an error. The card is not or could not be enrolled. It is ineligible for 3-D Secure processing.

CARD/CARDHOLDER ENROLLED (Y)

If the cardholder is enrolled the PaReq and AcsUrl will be returned in the result.

Step 1:
The merchant sends an HTTP post to ACSUrl.

Field Name	Value
PaReq	The PaReq returned by the Verify Enrollment Transaction
MD	Merchant Identifier. This value will be returned to the TermUrl

TermUrl	Merchant defined URL. The ACS will redirect back to this URL after authentication. The response will include the following fields: PaRes and MD.

Example:

```
<form name="AcsUrlForm" method="post" action="<AcsUrl> ">
   <input name="PaReq" type="text" size="50" value=" <PaReq>" />
   <input name="MD" type="text" size="50" value="<Merchant Identifier>" />
   <input name="TermUrl" type="text" size="50" value="<TermUrl>" />
  <input type="submit" />
</form>
```

Step 2:

The ACS redirects the cardholder back to the TermUrl. Included are the MD and PaRes. The merchant submits the verify transaction id and PaRes to the ThreeDSaleTransactions or ThreeDAuthorizeTransactions API.

CARD/CARDHOLDER NOT ENROLLED(N)

The merchant submits the verify transaction id and an *empty* PaRes to the ThreeDSaleTransactions or ThreeDAuthorizeTransaction API.

UNABLE TO VERIFY ENROLLMENT(U)

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

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 Card/Cardholder Not Enrolled(N).
2. If Card/Cardholder enrolled(Y) the PaRes must be included in the transaction request.

OPERATION END-POINT

The URL to submit 3D Sale transactions is as follows:
http://<domain>/merchants/<merchantid>/ThreeDSaleTransactions

The URL to submit 3D Authorize transactions is as follows:
http://<domain>/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
PaRes	Required if the Enrollment Status is Card/Cardholder enrolled(Y).	

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

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"
}
```

APPENDIX A – TRANSACTION STATE TYPES

Sale
Authorize
Capture
Void
Refund
Chargeback
Credit
CBK1
Verify
Recurring

APPENDIX B – TRANSACTION STATE TYPES

Successful
Error
Declined
Pending
Scrubbed
Fraud
Unconfirmed