Modirum MPI

Version 4.0.2.54

Merchant Interface v4

June 25, 2018

Copyright © 2006-2017 Modirum Ltd, 2017-2018 by VPOS Ltd.
The document may not be published or disclosed to a third party without the written permission of VPOS Ltd.

Disclaimer

Modirum disclaims all warranties and conditions with regard to the Products described in this document or other Modirum products, including all warranties and conditions of merchantability, whether express, implied or statutory, fitness for a particular purpose, title and non-infringement.
Modirum does not warrant that the Product shall satisfy customers' specific requirements, or that copies of the Product other than those provided or authorized by the Modirum shall possess functional integrity. Also, Modirum makes no warranties with respect to the fitness and operability of modifications not made by Modirum.
Modirum makes no warranties as to the accuracy of the information in this document. The information is based on the knowledge and information available in the time of issue and is subject to change without any notice.

Liability

In no event shall Modirum be liable for any loss or damage to revenues, profits or other incidental, indirect and consequential damage of any kind, resulting from use of Product or Product's performance.

Contact

Any inquiries relating to this document should be directed to:
VPOS Ltd
Narva mnt. 5-58,
Tallinn 10151
Estonia
Tel: +372 6444 205
Fax: +372 663 1100
E-mail: support@modirum.com

Copyright © 2006-2017 Modirum Ltd, 2017-2018 by VPOS Ltd.
The document may not be published or disclosed to a third party without the written permission of VPOS Ltd.

Contents

Contents....3

Tables....4

1 Introduction....5
1.1 Prerequisites....5
1.2 3-D Secure Protocol Documentation....5
1.3 Glossary....5
1.4 Getting Started....6
Creating Transaction....7

2 HTTP POST Interface....10
2.1 Parameters of the Post to MPI Server....10
2.1.1 Start or process an authentication session....10
2.1.2 Query authentication results....17
2.2 Calculation of the Signature....17
2.3 Redirection to ACS....18
2.4 Returning from MPI Server to Merchant Site....18
2.5 Parameters of return POST from MPI Server....18
2.6 Modirum MPI Transaction End Status....20
`mdStatus` and `eci` fields....20
Fully Authenticated Transactions....20
Non-participation and Not Enrolled Transactions....21
Attempts....21
Authentication Errors....21
Authentication Unavailable....21
3-D Secure Errors....22
Merchant data errors....22
System, networks or directory errors....22
Fraud Score Block....22
Pending Transactions....23
Summary....23

3 XML Interface....25
3.1 XML Parameters to be posted to MPI Server....25
3.2 Calculation of the Signature....32
3.3 XML parameters to be returned to Merchant....34
3.4 XML interface example....36

4 SOAP interface....43
4.1 SOAP interface example....43

Copyright © 2006-2017 Modirum Ltd, 2017-2018 by VPOS Ltd.
The document may not be published or disclosed to a third party without the written permission of VPOS Ltd.

Tables

Table 1 Glossary....6
Table 2 HTTP POST parameters for authentication session....17
Table 3 HTTP POST parameters for query service....17
Table 4 Parameters of return POST from MPI Server....19
Table 5 descriptions....24
Table 6 XML request parameters....32
Table 7 XML response parameters....35

Copyright © 2006-2017 Modirum Ltd, 2017-2018 by VPOS Ltd.
The document may not be published or disclosed to a third party without the written permission of VPOS Ltd.

1 Introduction

Modirum has developed a range of software products to support the use of 3-D Secure protocol for payer authentication. Modirum MPI is a product that is developed for merchants, acquirers or payment service providers that want to implement the 3-D Secure Merchant Plug-In (MPI) protocol. Modirum MPI is compliant with Visa, MasterCard, American Express, Diners and JCB schemas (protocol version 1.0.2). Since this version 4.0.2.51 also ThreeDSecure 2.0 and 2.1 support has been established. As of now 2.0 is discontinued and 2.1 protocol is pending yet certification.
This document is the reference manual of Modirum MPI merchant interface. It has been targeted to merchants who connect to and process 3D Secure through Modirum MPI
The structure of this document is as follows:

- Section HTTP POST Interface describes the merchant application interface of the product. The interface enables implementation of 3-D Secure protocol without any programming work. This section includes a separate summary of different result values of the 3-D Secure process (mdStatus, eci).

The new interface specification introduces recently emerged new MPI extension such as Brazil Market and Trusted Third Party and ThreeDSecure 2.x specifics and extensions. Please check for new fields in this version to ensure compability (look for “Since 4.0.2.54”)

1.1 Prerequisites

It is assumed that the reader has basic knowledge of payment cards in the traditional commerce and in electronic commerce. It is also assumed that the reader has basic knowledge about the acquiring process of the payment cards.

1.2 3-D Secure Protocol Documentation

Every 3-D Secure component must comply with the requirements of the core protocol, described in:

- 3-D Secure: Protocol Specification – Core Functions, Visa Publication 70000-01 (licensed)
- SPA Algorithm for the MasterCard Implementation of 3-D Secure, v 1.03, MasterCard Publication
- In addition, 3-D Secure Merchant Plug-In must comply with the following description of the functional requirements:
- 3-D Secure: Functional Requirements – Merchant Server Plug-in, Visa Publication 70003-01 (licensed)
- Any 3-D Secure component that supports mobile devices must also comply with the specifications for the supported extension:
- 3-D Secure Protocol Specification – Extension for Mobile Internet Devices, Visa Publication 70006-01 (licensed)
- Modirum MPI is compliant with the Extension for Mobile Internet Devices.
- The following documents are also related to the implementation of a Visa 3-D Merchant Plug-In:
- 3-D Secure: Functional Specification – Chip Card Authentication, Visa Publication 70005-01 (licensed)·
- 3-D Secure: Implementation Guide – Merchant, Visa Publication 70020-01·
- V.I.P. System BASE I Technical Specifications, dated 30 June 2000, Visa Publication 0844A-02
- Card Technology Standards Manual, dated April 1, 1997, Visa Publication 0534-01
- Visa International Account Information Security Standards Manual, version 1.4
- The TLS [Transport Layer Security] Protocol, version 1.0, dated January 1999, available at http://www.ietf.org/rfc/rfc2246.txt

Copyright © 2006-2017 Modirum Ltd, 2017-2018 by VPOS Ltd.
The document may not be published or disclosed to a third party without the written permission of VPOS Ltd.

1.3 Glossary

This section includes selected terms that are commonly used in the document. An extensive 3-D Secure glossary is available in 3-D Secure: System Overview, available through the "Vendors & Merchants" link on http://corporate.visa.com.

ACS =Access Control Server	A component that operates in the Issuer Domain, verifies whether authentication is available for a card number, and authenticates specific transactions.
API	Application Programming Interface
HTML	HyperText Markup Language
MDpay MPI Manager/Admin Tool	User interface implementation of the MDpay MPI database. The tool can be used to maintain merchant and directory server data as well as to browse transactions.
Merchant Plugin	A component that operates in the Acquirer Domain; incorporated into the merchant's Web storefront to perform functions related to 3-D Secure on behalf of the merchant, such as determining whether authentication is available for a card number and validating the digital signature in a 3-D Secure message.
MPI	See Merchant Plug-in.
PAN	Primary Account Number – often referred to as card number
PATransReq	Payer Authentication Transaction Request; a record of authentication activity sent by the ACS to the Authentication History Server
PATransRes	Payer Authentication Transaction Response; Authentication History Server response to PATransReq
PAReq = Payer Authentication Request	A message sent from the Merchant Server Plugin to the Access Control Server via the cardholder device. Requests the issuer to authenticate its cardholder and contains the cardholder, merchant, and transaction-specific information necessary to do so.
PARes = Payer Authentication Response	A message formatted, digitally signed, and sent from the Access Control Server to the Merchant Server Plug-in (via the cardholder device) providing the results of the issuer's 3D Secure cardholder authentication.
VEReq = Verify Enrollment Request	A message from the Merchant Server Plug-in to the Visa Directory or from the Visa Directory to the ACS, asking whether authentication is available for a particular card number
VERes = Verify Enrollment Response	A message from the ACS or the Visa Directory, telling the Merchant Server Plug-in whether authentication is available
Directory Server	A server hardware/software entity which is operated in the Interoperability Domain; it determines whether authentication is available for a specific card number, and if so, it returns the URL of the appropriate Access Control Server to the Merchant Server Plugin.
WAP	Wireless Application Protocol
WML	Wireless Markup Language
3DS Server	A server component used in ThreeDSecure 2.x that resempbles somewhat MPI functionality of ThreeDSecure 1.0 and is responsible with communications and interfacing with Directories and 3DS Requestors and ACS redirections in browser and redirection mode.
3DS Requestor	A end entity or Merchant participating in 3DS Secure 2.x protocol.
AReq	Authentication request in 3DS 2.x protocol
ARes	Authentication response in 3DS 2.x protocol
RReq	Results request in 3DS 2.x protocol
RRes	Results request response in 3DS 2.x protocol
CReq	Challenge request in 3DS 2.x protocol
CRes	Challenge request response in 3DS 2.x protocol

Table 1 Glossary

Copyright © 2006-2017 Modirum Ltd, 2017-2018 by VPOS Ltd.
The document may not be published or disclosed to a third party without the written permission of VPOS Ltd.

1.4 Getting Started

The purpose of this section is to describe the basic functionality of Modirum MPI. Functions of the product are walked-through with help of examples. More detailed description of the product is included in the rest of the document.
Note that the examples can be tested with a demo merchant and a live Modirum MPI. In order to get access to Modirum demo site, please contact Modirum support.
In order to try the following examples with Modirum software, please note the following recommendations:

- With the example merchant application, it is recommended to use FireFox, Chrome, or Internet Explorer 9 (or newer). The software has also been tested with other browsers, but there have been some technical problems with earlier browser versions.
- It is highly recommended to use a display with a minimum 1024x786 graphics resolution.

In the following examples, URLs are used to activate the demo and MPI Merchant Admin Tool. <hostname> refers to the server address that is used. It should be replaced with the actual IP address or server name.
Example:

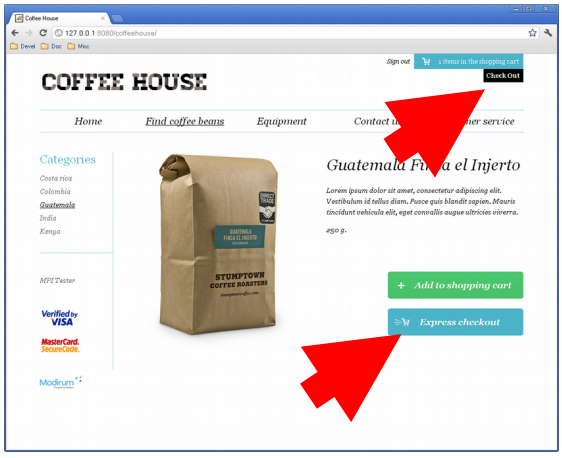
If the test server is installed to the address testserver.testmerchant.com
https://<hostname>/mpimngr/login/login.html

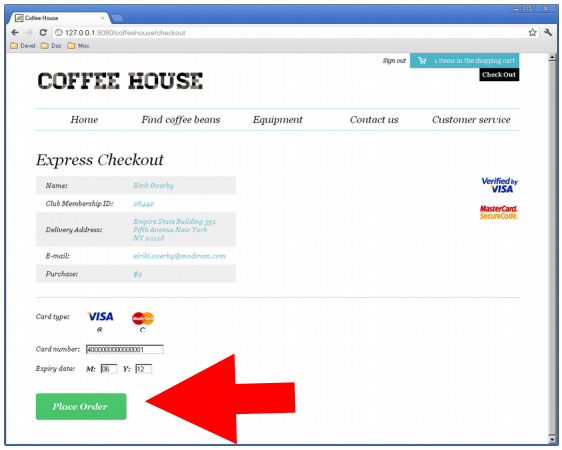
should be replaced with
https://testserver.testmerchant.com/mpimngr/login/login.html

In the following example, a card payment is done with the help of a demo application.

Creating Transaction

The demo starts from a merchant main page, which includes selection of coffee beans. The demo can be invoked from the address:
http://<hostname>/coffeehouse/
Note that the example shop is included in the software distribution and it can be installed to your own MDpay MPI installation. The merchant page can be activated similarly by changing the <hostname> to point at your server. However, you need to have access to Modirum test directory server and ACS (acs.modirum.com) to run a full transaction. Also, the default merchant (CoffeeHouse /1) and the directory server entry need to exist in the MPI database (data will be initialized, when the default database is created).





You can invoke Modirum MPI functionality and 3-D Secure protocol with the following steps:

- Press “Express Checkout” in the main screen
- Press “Express Checkout” in the shopping cart
- Input card number and expiry date in the Checkout Page and press “Place order”. You can get your own test card number from Modirum support.
- By default the demo shop is configured to use one of the modirum demo mpi/acs.
- To confirgure it to use Your mpi change in application installation directory
- WEB-INF\config\settings.default.yml line 20

Copyright © 2006-2017 Modirum Ltd, 2017-2018 by VPOS Ltd.
The document may not be published or disclosed to a third party without the written permission of VPOS Ltd.

- `"action: ‘https://3ds-acs.test.modirum.com:9601/mdpayacs/vereq'"`
- to point your MPI installation location

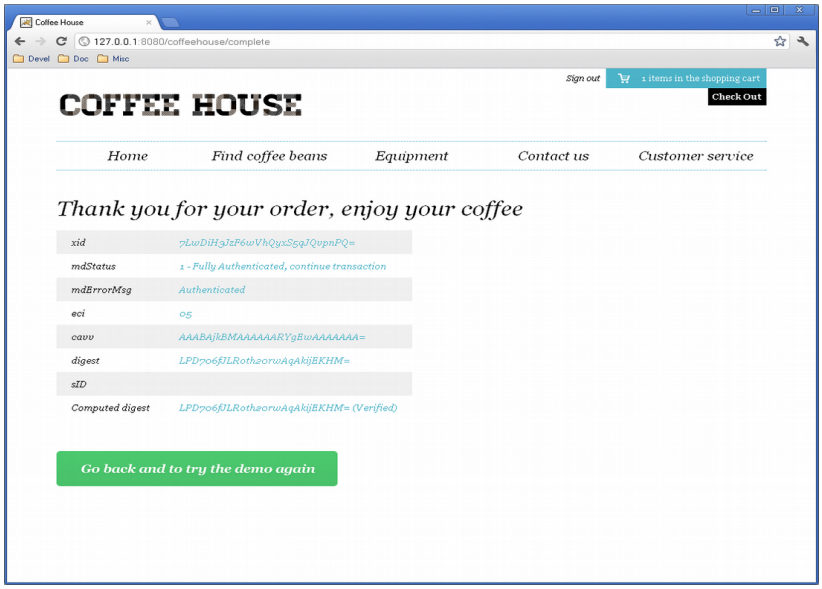
Before starting the 3-D Secure process, the following steps take place:

- Test merchant page activates the 3-D Secure Merchant Plug-In (MPI) by generating a HTTP POST to the Modirum MPI.
- The MPI connects to a 3-D Secure directory server to determine, if the card is enrolled and to get the url-address of the issuers Access Control Server (ACS). In the demo installation, Modirum test directory server is used.
- The MPI sends a Payment Authentication Request through the cardholder browser (redirected POST). The ACS receives the message.
- The ACS activates the cardholder authentication user interface (in case the card was enrolled and not blocked)

The cardholder user authentication user interface is a simple screen to input the 3-D Secure password. The screen also includes information about the transaction.

In the cardholder authentication screen, the cardholder must enter the password. After input of the password, the control moves back to the merchant system. If the ACS accepted the password, the test merchant application will confirm the successful transaction. Otherwise the merchant page informs about a failed transaction. The cardholder can also change password or cancel the transaction. Canceling the cardholder authentication will always result in Authentication Failed message to the merchant. In a production environment, the merchant would continue the process with a normal authorization.

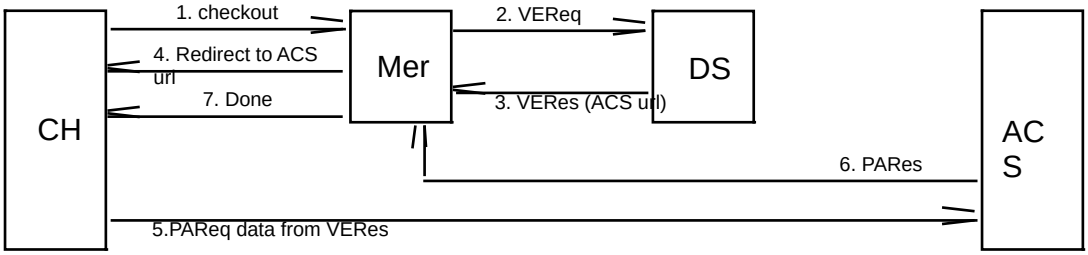
Copyright © 2006-2017 Modirum Ltd, 2017-2018 by VPOS Ltd.
The document may not be published or disclosed to a third party without the written permission of VPOS Ltd.



You can continue with new transactions by pressing Go back and try the demo again button in the final page.

Copyright © 2006-2017 Modirum Ltd, 2017-2018 by VPOS Ltd.
The document may not be published or disclosed to a third party without the written permission of VPOS Ltd.

2 HTTP POST Interface



3DS flow diagram

The simplest way to add 3-D Secure support to existing Merchant site is to use HTTP Post interface of the Modirum MPI.
The control flow using HTTP Post interface is the following:

1. Merchant payment page asks the user all the relevant payment data, such as card number, expiry, etc.
2. Merchant payment page calculates digest (version 3.0 or earlier) or the signature (v 4.0, detailed below) of all the fields to be posted to MDpay MPI including the shared secret (version 3.0 or earlier) and POSTs these fields except the shared secret to the Modirum MPI..
3. Modirum MPI checks the card participation from the 3-D Secure directory and return the redirection page to the Issuer ACS. The right directory is found with either card scheme id or matching the beginning of the card number.
4. After the ACS is finished with the user authentication, ACS returns the control to the Modirum MPI. The MPI Server verifies the signature of ACS and POSTs the response to either success URL or fail URL, which the MPI has earlier passed to the ACS.
5. Merchant payment page reads the response and continues with the authorization of the payment (or does the error processing).

2.1 Parameters of the Post to MPI Server

2.1.1 Start or process an authentication session

The following table describes the parameters of the POST from the payment page to Modirum MPI.
HTTP POST interface version has been upgraded to 4.0. The software still supports 3.0, 2.0 and 1.0 but it is not recommended to use version 2.0 or 1.0 as they will soon be deprecated.

Field **General parameters**	**Required / Optional**	**Description**
version	R	Version of MDpay MPI HTTP POST protocol. Allowed values 2.0 (soon to be deprecated), 3.0, 4.0 (only 4.0 has been documented in this section).
cardType	O/R	Card scheme can be defined explicitly. Values with one digit are valid. The value is matched to directory server entry that is mapped to the merchant with that particular cardType The field can also be left empty, which means that the directory server is determined from the card number. Required if panMode parameter value is MDESToken
pan	R	Card number. 13-19 digit account number
expiry	R	Expiration Date supplied to the merchant by cardholder (YYMM). Note that this field is not checked in most of the production ACS installations.
deviceCategory	R	Integer length 1, Indicates the type of cardholder device. Supported values are: 0 = www 1 = legacy mobile (deprecated, means wml interfaces) 4 = dtv (deprecated) 5 = mobile SDK (for ThreeDSecure 2.x only) 6 = for ThreeDS Requestor initiated (3RI) flow (for ThreeDSecure 2.x only) Since version 4.0.2.37 this field is required. Most cases this value shall be always 0 as wap phones are no longer mainstream and may not be supported by ACSes.

Copyright © 2006-2017 Modirum Ltd, 2017-2018 by VPOS Ltd.
The document may not be published or disclosed to a third party without the written permission of VPOS Ltd.

purchAmount	R	Max. 12-digit numeric amount in minor units of currency with all punctuation removed. Examples: Display Amount USD 123.45 Purchase Amount 12345
exponent	R	Exponent number length 1 The minor units of currency specified in ISO 4217. For example, US Dollars has a value of 2; Japanese Yen has a value of 0.
description	O	Purchase description. Brief description of items purchased, determined by the merchant. Maximum size is 125 characters, but merchant should consider the characteristics of the cardholder's device when creating the field. Note: Most Issuers do not display the description to the user.
currency	R	Currency. Determined by merchant. ISO 4217, 3 digit numeric.
merchantID	R	ID to identify the merchant to MDpay MPI.
merchantName	O	**Length**: 1-25 characters **Format**: any characters Send this parameter if you want to override PAReq.Merchant.name. By default it is taken from mpi database
xid	R	Unique transaction identifier determined by merchant. Contains a 20 byte statistically unique value that has been Base64 encoded, giving a 28 byte result.
okUrl	R	Fully qualified URL to Merchant. MDpay MPI will do POST when finished to this URL in all other cases, except when authentication or signature validation fails (mdStatus=0). Max length 2048 chars Not applicable if deviceCategory=5 or 6
failUrl	R	Fully qualified URL to Merchant. MDpay MPI will do POST to this URL when authentication or signature validation fails. mdStatus=0. Max length 2048 chars Not applicable if deviceCategory=5 or 6
MD	O	The MD ("Merchant Data") field: merchant state data that must be returned to the merchant. The content of this field is passed unchanged and without assumptions about its content to the return POST. This field is used to accommodate the different ways merchant systems handle session state. If the merchant system can associate the final post with the original shopping session without any further assistance, the MD field may be empty. If the merchant system does not maintain state for a given shopping session, the MD can carry whatever data the merchant needs to continue the session. This field must contain only ASCII characters in the range 0x20 to 0x7E; **Since version 4.0.2.15 characters '<' and '>' are not allowed in this parameter.** If other data is needed, the field must be Base64 encoded. The size of the field (after Base64 encoding, if applicable) is limited to 254 bytes. If MD includes confidential data (such as the PAN), it must be encrypted.
recurFreq	O	Recurring frequency for PAReq/AReq Purchase.Recur.frequency (integer days, 28 means monthly)
recurEnd	O/R	Recurring end date for PAReq/AReq format YYYYMMDD, If recurFreq is present then recurEnd is required
installments	O	Number of Installments for PAReq/AReq.Purchase.install integer value >1 and <=999. I**nstall and recurring parameters can not be present at the same time.**
panMode	O	Possible values: **MDESToken** – to indicate that instead of real pan pan parameter will contain MasterCard Digital Enablement Service Token
Brazil Market extension parameters		
brazilmcc	O/R	Required if Brazil extension is used. Merchant Category Code, provided by the merchant (Length – 1-4, Numeric digits)

Copyright © 2006-2017 Modirum Ltd, 2017-2018 by VPOS Ltd.
The document may not be published or disclosed to a third party without the written permission of VPOS Ltd.

brazilaccounttype	O/R	Required if Brazil extension is used. Account Type (as selected by the cardholder during checkout) (Length – 1-2, Numeric digits) Code Definitions 00 NOT APPLICABLE 01 CREDIT 02 DEBIT 03 VISA VALE REFEIÇÃO 04 VISA VALE ALIMENTAÇÃO
brazilmobilenumber	O/R	Required if Brazil extension is used. Mobile Number (as entered by the cardholder during checkout) (Length – 1-25, Numeric digits)
braziltransactiontype	O/R	Required if Brazil extension is used. Transaction Type, provided by the merchant (Length – 1-2; Numeric Digit) Code Definitions 00 Goods / Service Purchase 03 Check Acceptance 10 Account Funding 11 Quasi-Cash Transaction 28 Prepaid Activation & Load
TrustedThirdParty extension parameters (TTP MasterCard)		
TTP.RiskDetermination.transactionID	O/R	Required if extension is used, to be filled as specified by extension
TTP.RiskDetermination.score	O/R	Required if extension is used, to be filled as specified by extension
TTP.RiskDetermination.scoreMin	O/R	Required if extension is used, to be filled as specified by extension
TTP.RiskDetermination.scoreMax	O/R	Required if extension is used, to be filled as specified by extension
TTP.RiskDetermination.Recommendation	O/R	Required if extension is used, to be filled as specified by extension
TTP.RiskDetermination.provider.ID	O/R	Required if extension is used, to be filled as specified by extension
TTP.RiskDetermination.provider.name	O/R	Required if extension is used, to be filled as specified by extension
TTP.Wallet.provider.ID	O/R	Required if extension is used, to be filled as specified by extension
TTP.Wallet.provider.name	O/R	Required if extension is used, to be filled as specified by extension
TTP.Wallet.TransactionTrustLevel	O/R	Required if extension is used, to be filled as specified by extension
TTP.Wallet.CardholderVerificationStatus	O/R	Required if extension is used, to be filled as specified by extension
TTP.Wallet.DeviceTrustLevel	O/R	Required if extension is used, to be filled as specified by extension
TTP.Wallet.SessionTrustLevel	O/R	Required if extension is used, to be filled as specified by extension
TTP.Wallet.transactionRefNumber	O/R	Required if extension is used, to be filled as specified by extension
TTP.Wallet.userProfileID	O/R	Required if extension is used, to be filled as specified by extension
TTP.Wallet.LoginMethodStrength	O/R	Required if extension is used, to be filled as specified by extension
TTP.Wallet.userAccountAge	O/R	Required if extension is used, to be filled as specified by extension
TTP.Wallet.accountTrustLevel	O/R	Required if extension is used, to be filled as specified by extension
TTP.Wallet.accountTrustLevelMin	O/R	Required if extension is used, to be filled as specified by extension
TTP.Wallet.accountTrustLevelMax	O/R	Required if extension is used, to be filled as specified by extension
TTP.Wallet.paymentCardAge	O/R	Required if extension is used, to be filled as specified by extension
SafeKey EA extension parameters		
SKEA.amountTransaction	O/R	Required when extension is present. 1-10 digits,numeric. Warning: if this value is not included then the extension will not be added.
SKEA.currencyCode	O/R	Required when extension is present. 3 digits (ISO 4217 3-digit numeric code)
SKEA.sellerType	O/R	Required when extension is present. 2 digit numeric value
SKEA.cmBillingFirstName	O/R	Required when extension is present.. 1-99 character alphanumeric value
SKEA.cmBillingMiddleName	O/R	Required when extension is present. 1-99 character alphanumeric value
SKEA.cmBillingLastName	O/R	Required when extension is present. 1-99 character alphanumeric value
SKEA.cmBillingPostalCode	O	5-20 digit numeric value
SKEA.cmBillingAddress	O	1-99 character alphanumeric value
SKEA.cmBillingCity	O	1-99 character alphanumeric value
SKEA.cmBillingState	O	2-99 character alphanumeric value
SKEA.cmBillingCountryCode	O	3 digit ISO 3166 numeric value
SKEA.registeredEmail	O/R	Required when extension is present. 6-99 valid email alphanumeric value
SKEA.registeredPhone	O	10-20 digit numeric value
SKEA.registeredPhoneCountryCode	O	2 digit numeric value

Copyright © 2006-2017 Modirum Ltd, 2017-2018 by VPOS Ltd.
The document may not be published or disclosed to a third party without the written permission of VPOS Ltd.

SKEA.countOfShipToAddressesOnFile	O	1-2 digit numeric value
SKEA.cmShippingFirstName	O	1-99 character alphanumeric value
SKEA.cmShippingMiddleName	O	1-99 character alphanumeric value
SKEA.cmShippingLastName	O	1-99 character alphanumeric value
SKEA.cmShippingPostalCode	O/R	Required if extension is present and shipping method is not electronic delivery (05). 5-20 digit numeric value
SKEA.cmShippingAddress	O/R	equired if extension is present and shipping method is not electronic delivery (05). 1-99 character alphanumeric value
SKEA.cmShippingCity	O	1-99 character alphanumeric value
SKEA.cmShippingState	O	2-99 character alphanumeric value
SKEA.cmShippingCountryCode	O	3 digit ISO 3166 numeric value
SKEA.shippingMethod	O/R	Required when extension is present and transaction is retail. 2 digit numeric value as detailed by the extension
SKEA.shippingTenure	O	8 digit numeric value
SKEA.electronicDeliveryEmail	O	6-99 character valid email address
SKEA.CartItem.1-9999.XXX	O	Cart items parameters. The segment after the first period determines the ordinal number of the cart item and the segment after the second period determines the parameter name. Numbering of cartItems starts from 1 and goes up to 9999. If ,for a given N, all of the parameters are null of empty, parameters for ordinals higher than N are not further processed. The exact parameters are detailed below.
SKEA.cartItem.N.sku	O	1-20 character alphanumeric value
SKEA.cartItem.N.desc	O	1-99 character alphanumeric value
SKEA.cartItem.N.price	O	1-10 digit numeric value
SKEA.cartItem.N.category	O	4 digit numeric value
SKEA.cartItem.N.qty	O	1-4 digit numeric value
SKEA.cartItem.N.attributes	O	1-99 character alphanumeric value
SKEA.IACTransaction.departureDate	O/R	Required if sellerType = 01 and transaction amount is $200 or more. Date string formatted as “yyyy-MM-dd’T’HH:mm:ss”
SKEA.IACTransaction.passenger.1-9999.XXX	O/R	Required if sellerType = 01 and transaction amount is $200 or more. The segment after the first period determines the ordinal number of the passenger and the segment after the second period determines the parameter name. Numbering of passengers starts from 1 and goes up to 9999. If ,for a given N, all of the parameters are null of empty, parameters for ordinals higher than N are not further processed.
SKEA.IACTransaction.passenger.N.firstname	O/R	1-99 character alphanumeric value
SKEA.IACTransaction.passenger.N.lastname	O/R	1-99 character alphanumeric value
SKEA.IACTransaction.origin	O/R	Required if sellerType = 01 and transaction amount is $200 or more. 3-5 character alphanumeric value
SKEA.IACTransaction.dest	O/R	Required if sellerType = 01 and transaction amount is $200 or more. 3-5 character alphanumeric value
SKEA.IACTransaction.airlineCarriers	O	1-40 character alphanumeric value
SKEA.IACTransaction.numberOfPassengers	O	1-5 digit numeric value
3DS 2.x SDK extra fields		
TDS2.sdkTransID	O/R	Required if deviceCategory=5 Length: 36 characters,Format: UUID
TDS2.sdkReferenceNumber	O/R	Required if deviceCategory=5 Length: 1-32 characters
TDS2.sdkAppID	O/R	Required if deviceCategory=5 Length: 36 characters,Format: UUID
TDS2.sdkEncData	O/R	Required if deviceCategory=5 Length: 1-64000 characters
TDS2.sdkMaxTimeout	O/R	Required if deviceCategory=5 Type: numeric Format: >= 05 Length: 2
TDS2.deviceRenderOptionsIF	O/R	Required if deviceCategory=5. deviceRenderOptions interface Format: numeric Length: 1-2

Copyright © 2006-2017 Modirum Ltd, 2017-2018 by VPOS Ltd.
The document may not be published or disclosed to a third party without the written permission of VPOS Ltd.

TDS2.deviceRenderOptionsUI	O/R	Required if deviceCategory=5 deviceRenderOptions UI Format: comma separated numeric values Length: 1-20 Example: 01,02,03 for >= 2.1.0 messageVersion 1,2,3 for < 2.1.0 messageVersion
TDS2.sdkEphemPubKey	O/R	Required if deviceCategory=5 Length: 1-260 If messageVersion: < 2.1.0, the length should be 128 and value is Base64 Encoded binary key If messageVersion: >= 2.1.0, the length should be 256 and value is semicolon separated Json Web Key components: Crv;kty;x;y Example: EC;P-256;z-gcYjDjK3ZP-lqZk4ixWP-gNAaFMkGLgdRwsSzlINk;xa-ufJNEgV1RFiEwQNQG0JtlGKcRDTT95S_mtzJ-f8s
3DS 2.x general extra fields		
TDS2.acctID	O	Variable string..64 extra account info
TDS2.acctType	O	Fixed str 2: 01 = Not Applicable, 02 = Credit, 03 = Debit
TDS2.addrMatch	O	Fixed string Y/N: Y = Shipping Address matches Billing Address. N = Shipping Address does not match Billing Address.
TDS2.cardholderName	O	Var string 2..45. Cardholder name
TDS2.email	O	Var string ..254
TDS2.homePhone	O	Var string ..19 (..3-..15): Home phone format cc-subscriber 1-686123456
TDS2.mobilePhone	O	Var string ..19 (..3-..15): Mobile phone format cc-subscriber 1-686123456
TDS2.workPhone	O	Var string ..19 (..3-..15): Work phone format cc-subscriber 1-686123456
TDS2.messageCategory	O	Fix string 2: 01 = PA(payment), 02 = NPA(non payment), defaults to 01
TDS2.messageVersion	O	In case it is required to force MPI to use particular message version for this transaction (in case MPI and Issuer supports it). If not supported then MPI will use one of supported messageVersion-s Format: 2.0.1 or 2.1.0 Length: 5. Mostly for specific testing only. Not recommended to be used as MPI resolves on its own appropriate version.
TDS2.purchaseDate	O/C	Purchase date in GMT: Format YYYYMMDDHHMMSS. Optional for normal purchases and will de defaulted to current time. Shall be present for installments and recurrings and set to original purchase agreement date .
TDS2.transType	O	Fix string 2 : 01 = Goods/ Service Purchase 03 = Check Acceptance, 10 = Account Funding, 11 = Quasi-Cash Transaction, 28 = Prepaid Activation and Load
TDS2.threeDSRequestor3RIInd	O	Fix string 2: Unsure its use case: 01 = Recurring transaction 02 = Installment transaction, 03 = Add card,04 = Maintain card information, 05 = Account verification. (this is field threeRIInd in case of 2.1), to be used only if deviceCategory=6.
TDS2.threeDSRequestorAuthenticationInd	O	Type: string Length: 2 Accepted values: 01 - Payment, 02 -recurring, 03 - instalment, 04 – add card??, 05 – maintain card??, 06 – verification as part token EMV token ID
TDS2.threeDSRequestorChallengeInd	O	Fix string 2. Challenge request prefrences indicator. 01 = No preference 02 = No challenge requested, 03 = Challenge requested: 3DS Requestor Preference, 04 = Challenge requested: Mandate
TDS2.threeDSRequestorID	O	Type: string Length: 1-35. Note: Normally filled by MPI from its configuration
TDS2.threeDSRequestorName	O	Type: string Length: 1-40 Note: Normally filled by MPI from its configuration
TDS2.threeDSRequestorNPAInd	O/R	Fix string 2, unsure of use case: 01 = Add card, 02 = Maintain card information, 03 = Cardholder verification as part of EMV token ID&V According to EMVCo 3DS Spec Required if TDS2.messageCategory is 02
TDS2.threeDSRequestorURL	O	Fully qualified URL of 3DS Requestor website or customer care site. If not provided, then url will be taken from merchant config in database. Length: Var string ..2048 Example: http://server.domainname.com

Copyright © 2006-2017 Modirum Ltd, 2017-2018 by VPOS Ltd.
The document may not be published or disclosed to a third party without the written permission of VPOS Ltd.

TDS2.challengeWindowSize	O	Desired challenge window size for 2.x. Number 2. Values accepted 01 = 250 x 400, 02 = 390 x 400, 03 = 500 x 600, 04 = 600 x 400, 05 = Full screen
TDS2.payTokenInd	O	Type: string Length: 4
TDS2.acquirerBIN	O	Type: numeric Length: 1-11
TDS2.acquirerMerchantId	O	Type: string Length: 1-35
TDS2.merchantName	O	Type: string Length: 1-40
TDS2.mcc	O	Type: numeric Length: 4
TDS2.merchantCountryCode	O	Type: numeric Length: 3
3DS 2.0 Merchant Risk fields		
TDS2.mriShipIndicator	O	Format 2 numeric characters, See table A.7.2 EMVCO spec
TDS2.mriDeliveryTimeframe	O	Type: numeric Length: 1-2
TDS2.mriDeliveryEmailAddress	O	Format up to 254 numeric characters eamil, See table A.7.2 EMVCO spec
TDS2.mriReorderItemsInd	O	Type: numeric Length: 1-2
TDS2.mriPreOrderPurchaseInd	O	Type: numeric Length: 1-2
TDS2.mriPreOrderDate	O	Format 8 character, date YYYYMMDD See table A.7.2 EMVCO spec
TDS2.mriGiftCardAmount	O	Format max len 15 numeric value in minor units.
TDS2.mriGiftCardCurr	O	Format 3 numeric characters ISO4217
TDS2.mriGiftCardCount	O	Format 2 numeric characters
3DS 2.0 extra account info fields		
TDS2.chAccAgeInd	O	Length of time that the cardholder has had the account with the 3DS Requestor. Format and values according to EMVCo specification
TDS2.chAccDate	O	Fix YYYYMMDD, Date that the cardholder opened the account at merchant
TDS2.chAccChangeInd	O	Length of time since the cardholder's account information with the 3DS Requestor was last changed. Including Billing or Shipping address, new payment account, or new user(s) added. Format and values according to EMVCo specification
TDS2.chAccChange	O	Fix YYYYMMDD, Date that the cardholder's account with the 3DS Requestor was last changed. Including Billing or Shipping address,
TDS2.chAccPwChangeInd	O	Length of time since the cardholder's account with the 3DS Requestor had a password change or account reset. Format and values according to EMVCo specification
TDS2.chAccPwChange	O	Fix YYYYMMDD, Date that cardholder's account with the 3DS Requestor had a password change or account reset.
TDS2.nbPurchaseAccount	O	Var num string ..4: Number of purchases with this cardholder account during the previous six months.
TDS2.provisionAttemptsDay	O	Var num string ..3: Number of Add Card attempts in the last 24 hours.
TDS2.txnActivityDay	O	Var num string ..3: Number of transactions (successful and abandoned) for this cardholder account with the 3DS Requestor across all payment accounts in the previous 24 hours.
TDS2.txnActivityYear	O	Var num string ..3: Number of transactions (successful and abandoned) for this cardholder account with the 3DS Requestor across all payment accounts in the previous year.
TDS2.shipAddressUsageInd	O	Indicates when the shipping address used for this transaction was first used with the 3DS Requestor. Format and values according to EMVCo specification
TDS2.shipAddressUsage	O	Fix YYYYMMDD, Date when the shipping address used for this transaction was first used with the 3DS Requestor
TDS2.shipNameIndicator	O	Type: numeric Length: 1-2
TDS2.paymentAccInd	O	Indicates the length of time that the payment account was enrolled in the cardholder's account with the 3DS Requestor. Format and values according to EMVCo specification

Copyright © 2006-2017 Modirum Ltd, 2017-2018 by VPOS Ltd.
The document may not be published or disclosed to a third party without the written permission of VPOS Ltd.

TDS2.paymentAccAge	O	Fix YYYYMMDD, Date that the payment account was enrolled in the cardholder's account with the 3DS Requestor.
TDS2.suspiciousAccActivity	O	Indicates whether the 3DS Requestor has experienced suspicious activity (including previous fraud) on the cardholder account. Type: numeric Length: 1-2
3DS 2.0 extra billing addres fields		
TDS2.billAddrCity	O	Var string ..50, City
TDS2.billAddrCountry	O	Fix num 3, country code 3166-1 numeric
TDS2.billAddrLine1	O	Var string ..50, Address line 1
TDS2.billAddrLine2	O	Var string ..50, Address line 2
TDS2.billAddrLine3	O	Var string ..50, Address line 3
TDS2.billAddrPostCode	O	Var string 16, Zip code
TDS2.billAddrState	O	Var str 2 3166-2 country subdivision code
3DS 2.0 extra shipping addres fields		
TDS2.shipAddrCity	O	Var string ..50, City
TDS2.shipAddrCountry	O	Fix num 3, country code 3166-1 numeric
TDS2.shipAddrLine1	O	Var string ..50, Address line 1
TDS2.shipAddrLine2	O	Var string ..50, Address line 2
TDS2.shipAddrLine3	O	Var string ..50, Address line 3
TDS2.shipAddrPostCode	O	Var string 16, Zip code
TDS2.shipAddrState	O	Var str 2 3166-2 country subdivision code
3DS 2.0 extra authentication info Information about how the 3DS Requestor authenticated the cardholder before or during the transaction.		
TDS2.AIAuthMethod	O	Fix num 2: 01 = No 3DS Requestor authentication occurred (i.e. cardholder "logged in" as guest) 02 = Login to the cardholder account at the 3DS Requestor system using 3DS Requestor's own credentials 03 = Login to the cardholder account at the 3DS Requestor system using federated ID 04 = Login to the cardholder account at the 3DS Requestor system using FIDO Authenticator
TDS2.AIAuthTimestamp	O	Date YYYYMMDDHHMM, Date and time in UTC of the cardholder authentication.
TDS2.AIAuthData	O	Var str 2048. Data that documents and supports a specific authentication process.
3DS 2.0 extra authentication info Information about how the 3DS Requestor authenticated the cardholder as part of a previous 3DS transaction.		
TDS2.PAIRef	O	Var sting 36. (threeDSReqPriorRef) This data element contains a ACS Transaction ID for a prior authenticated transaction
TDS2.PAIAuthMethod	O	Fir num 2. (threeDSReqPriorAuthMethod) Mechanism used by the Cardholder to previously authenticate to the 3DS Requestor. 01 = Frictionless authentication occurred by ACS 02 = Cardholder challenge occurred by ACS
TDS2.PAIAuthTimestamp	O	Date YYYYMMDDHHMM UTC. Date and time in UTC of the prior cardholder authentication.
TDS2.PAIAuthData	O	Var strr 2048. (threeDSReqPriorAuthData) Data that documents and supports a specific authentication process.
Additional fields since 3DS 2.1.0		
TDS2.broadInfo	O	Type: string representing a JSON Object Length: 2-4096 If not JSON object then in case of 2.1 value is converted to JSON object as {"value" : "value of field" } and passed as is only in case 2.0. (Backward compability behavior)
3DS 2.0 extra message extensions (up to 100 extensions. Each extension parameter set comes with sequence number N. For example TDS2.ME.1.paramname1, TDS2.ME.1.paramname2, …)		
TDS2.ME.{N}.name	O	The name of the extension data set as defined by the extension owner. Var string ..64
TDS2.ME.{N}.id	O	A unique identifier for the extension. Var string ..64

Copyright © 2006-2017 Modirum Ltd, 2017-2018 by VPOS Ltd.
The document may not be published or disclosed to a third party without the written permission of VPOS Ltd.

TDS2.ME.{N}.criticalityIndicator	O	A Boolean value indicating whether the recipient must understand the contents of the extension to interpret the entire message. true/false
TDS2.ME.{N}.data	O	The data carried in the extension. A JSON object Var string ..8059 If not JSON object then in case of 2.1 value is converted to json object {“value” : “value of the field” } and passed as us only in case 2.0. (Backward compability behavior)
signature	R	Base64 encoded value of signature (RSA with SHA2-256) of all the field values above concatenated together having “;” semicolon in between (including trailing semicolon after the last value). signature=base64(RSA with SHA2-256(utf8bytes(value1;value2;...;value n;))) If missing or mismatching error is displayed and request in not further processed

Table 2 HTTP POST parameters for authentication session

2.1.2 Query authentication results

This interface makes it possible to ask for the the status of already processed authentication in MPI

Field **General parameters**	**Required / Optional**	**Description**
version	R	Version of MDpay MPI HTTP POST protocol. Allowed values 3.0 and 4.0 (only 4.0 has been documented in this section
merchantID	R	ID to identify the merchant to MDpay MPI.
service	R	Value: statusQuery
format	R	Valid values:for application/x-www-form-urlencoded format
xid	R	Unique transaction identifier determined by merchant to query. Contains a 20 byte statistically unique value that has been Base64 encoded, giving a 28 byte result.
signature	R	Base64 encoded value of signature (RSA with SHA2-256) of all the field values above concatenated together having “;” semicolon in between (including trailing semicolon after the last value).Signature=base64(RSA with SHA2-256(utf8bytes(value1;value2;...;value n;))). If missing or mismatching, error is displayed and the request is not further processed.

Table 3 HTTP POST parameters for query service

2.2 Calculation of the Signature

The digest in the incoming POST and in the return POST is calculated by the following rule.

1. Concatenate all the values of all the possible fields **with semicolon “;” in between** (including trailing semicolon after the last value) as listed and in same order as in the table. If a parameter is missing (not sent) or sent value is empty string “”, then value and separator is not concatenated.
2. Calculate RSA with SHA2-256 signature of step 1 (using of UTF-8 char encoding when converting string to bytes) using your private key.
3. Return the signature in base64 encoded form
4. Notes: Never implement the signature calculation in the browser using javascipt or similar as this way you expose your private key to the world. Only implement it on server side executed code as (jsp/servlet/asp/php etc).

For example:
Signature=base64(RSA with SHA2-256(utf8bytes(value1;value2;...;value n;)))

Example code for Java users:

```
java.security.PrivateKey privateKey = getPrivateKey(); //fetch your private key
```

Copyright © 2006-2017 Modirum Ltd, 2017-2018 by VPOS Ltd.
The document may not be published or disclosed to a third party without the written permission of VPOS Ltd.

```
java.security.Signature signature = Signature.getInstance("SHA256withRSA");
signature.initSign(privateKey);
signature.update(concatenatedValues.toString().getBytes(StandardCharsets.UTF_8));
byte[] sigBytes=signature.sign();
String sigStr=Base64.encode(sigBytes);
```

Example for .Net users:

```
System.Security.Cryptography.SHA256 sha = new System.Security.Cryptography.SHA256CryptoServiceProvider();
byte[] hashValue = sha.ComputeHash(System.Text.Encoding.UTF8.GetBytes(valueToDigest));
string digest = System.Convert.ToBase64String(hashValue);
CODE FOR SIGNATURE GENERATION TO BE ADDED HERE
```

2.3 Redirection to ACS

The MPI Server generates a redirection page, which includes a form that is posted to the ACS. The format of this page depends on the channel. PAReq redirection-templates of different channels are defined in the **mpi.properties** file.

Note: Normally the end user does not need to do anything with those templates and leave them as is packaged with MPI so this section details are removed.

2.4 Returning from MPI Server to Merchant Site

The standard method for returning control back from the MPI Server to the merchant is a redirection through the user browser.

The standard control flow after receiving the PARes (or CPRS with condensed messages) is:

1. ACS Posts the PARes back to MPI Server via the user browser using the redirection
2. MPI Server determines the status of the transaction and posts the status values to merchant payment page via the user browser using the redirection
3. Merchant server continues with authorization and after the authorization displays the confirmation page to the user.

2.5 Parameters of return POST from MPI Server

The following table describes the parameters of the POST to okURL or failURL by Modirum MPI.

Field	Required / Optional	Description
version	R	Version of MDpay MPI HTTP POST protocol. Copied from the HTTP POST request. Currently 4.0, 3.0 3 digit alphanumeric
merchantID	R	From merchantID field of the incoming POST
xid	R	From xid field of the incoming POST
mdStatus	R	End status of the transaction mdStatus field provides all the information that is needed to determine, how to manage the transaction in the merchant system See section 2.6 Modirum MPI Transaction mdStatus
mdErrorMsg	R	Up to 128 bytes alphanumeric description of the error.
veresEnrolledStatus	R	The actual value of veres enrollement status like "Y", "N", "U" or "-" if value is not available due errors etc. (since 4.0.2.31). **Note:** In case of UPOP protocol this value is always Y except status response code 77.
paresTxStatus	R	The actual value of pares tx status "Y", "N", "U", "A", “C”, “R” or "-" if value is not available due errors or not enrolled. (since 4.0.2.31) **Note:** In case of UPOP protocol this value is equal to **activateStatus** (Y,A,F,L,N) if respCode is 00. - in case respcode 77 and ant other respcode cases N (not authenticated).
iReqCode	O	Two digit numeric code provided by ACS indicating data that is formatted correctly, but which invalidates the request. This element is included when business processing cannot be performed for some reason. Never provided if mdStatus=0. 3-D Secure iReqCode field. **Note:** In case of UPOP protocol this value is equal to **respCode** if respCode is not 00.

Copyright © 2006-2017 Modirum Ltd, 2017-2018 by VPOS Ltd.
The document may not be published or disclosed to a third party without the written permission of VPOS Ltd.

iReqDetail	O	May identify the specific data elements that caused the Invalid Request Code (so never supplied if Invalid Request Code is omitted). See Table 20 on page 60 for details. Note: In case of UPOP protocol this value is equal to respMsg if respCode is not 00.
vendorCode	O	Error message describing iReqDetail error.
eci	O	Electronic Commerce Indicator With Visa cards, the value to be passed in Authorization Message (exactly 2 decimal digits). ECI fields determine the final status of the transaction See section 2.6 Modirum MPI Transaction mdStatus
cavv	O	Cardholder Authentication Verification Value Determined by ACS. Contains a 20 byte value that has been Base64 encoded, giving a 28 byte result. Some Visa regions may require that this value be included in the VIP authorization message (Visa EU is not using CAVV as of 10.10.02). **Note:** In case of UPOP protocol this value is equal to UPOP **vcode**.
cavvAlgorithm	O	A positive integer indicating the algorithm used to generate the Cardholder Authentication Verification Value. Current defined values are: 0 = HMAC (as per SET™ TransStain) 1 = CVV 2 = CVV with ATN 3 = MasterCard AAV Note that the value is copied directly from the PARes/RReq message.
MD	O	From MD field of the incoming POST
PAResVerified	O	If signature validation of the return message is successful, the value is true. If PARes message is not received or signature validation fails, the value is false. (Compliance testing facility requirement). If signature validation is omitted the value will be empty In case of 2.x there is no signatures but signature valid flag is set to true for backward compability, as data is trusted from mutual TLS authentication.
PAResSyntaxOK	O	If PARes validation is syntactically correct, the value is true. Otherwise value is false. (Compliance testing facility requirement)
protocol	O	Protocol used in processing eg: 3DS1.0.2, 3DS2.1.0 , SP5 Will be present if processing started. **Note: new Since 4.0.1.54**
cardType	O	Card type resolved by MPI if not in request or same value as in request.. **Note: new Since 4.0.1.54**
3DS 2.x general and SDK fields		
TDS2.sdkTransID	-/R	Required if deviceCategory=5 Length: 36 characters, Format: UUID
TDS2.transStatus	O/C	Required if available
TDS2.transStatusReason	O/C	Required if available Since 4.0.2.54
TDS2.threeDSServerTransID	O/C	Required if available
TDS2.dsTransID	O/C	Required if available
TDS2.acsTransID	O/C	Required if available
TDS2.acsRenderingType	O/C	Required if available
TDS2.acsReferenceNumber	O/C	Required if available
TDS2.acsSignedContent	O/C	Required if available and request deviceCategory=5
TDS2.authTimestamp	O/C	Required if available YYYYMMDDHHMM, 3DSServer set timestamp of authentication received in GMT (may change in future)
TDS2.messageVersion	O/C	3DS Message version used. (example 2.1.0 or 2.0.1) Since 4.0.2.54
TDS2.acsChallengeMandated	O/C	Required if available Since 4.0.2.54
TDS2.authenticationType	O/C	Required if available Since 4.0.2.54
TDS2.acsOperatorID	O/C	Required if available Since 4.0.2.54
TDS2.cardholderInfo	O/C	Required if available. If provided. Merchant shall show contents of this field to cardholder. Since 4.0.2.54
TDS2.acsUrl	O/C	Required if available Since 4.0.2.54 (In SDK mode this is already contained in acs signed content)
signature	R	Base64 encoded value of signature (RSA with SHA2-256) of all the field values above concatenated together having ";" semicolon in between (including trailing semicolon after the last value).Signature=base64(RSA with SHA2-256(utf8bytes(value1;value2;...;value n;))). If missing or mismatching, do not continue to payment as may be counterfeit or error message

Copyright © 2006-2017 Modirum Ltd, 2017-2018 by VPOS Ltd.
The document may not be published or disclosed to a third party without the written permission of VPOS Ltd.

Table 4 Parameters of return POST from MPI Server

Note: In case of deviceCategory=5 then no html is returned but name value pairs content only in application/x-www-form-urlencoded format. Response to service query also returns this set of parameters in application/x-www-form-urlencoded format.

2.6 Modirum MPI Transaction mdStatus

mdStatus and eci fields

Mdpay MPI returns many fields in the HTTP POST return interface, but there are two fields that have the most significance from business transaction management point of view.

- mdStatus field provides all the information that is needed to determine, how to manage the transaction in the merchant system:
  - 0 = Not Authenticated, do not continue transaction
  - 1 = Fully Authenticated, continue transaction
  - 2 = Not enrolled
  - 3 = Not enrolled cache
  - 4 = Attempt
  - 5 = U-received
  - 6 = Error received (from Directory or ACS)
  - 8 = Block by Fraud Score (not used currently)
  - 9 = Pending (this code is not sent internal only except SDK in challenge)
  - 50 = Execute 3D method and continue to authentication (XML API(SOAP only).
  - 80 = Skip device case (no 3DS performed as device known not well capable)
  - 91 = Network error
  - 92 = Directory error (read timeout)
  - 93 = Configuration error
  - 94 = Merchant input errors
  - 95 = No directory found for PAN/cardtype
  - 96 = No version 2 directory found for PAN/cardtype
  - 99 = System error (our error)

- eci field is relevant in Visa infrastructure, because there are certain business rules of how to fill the field into the authorization messages. However, in Modirum MPI, eci field is filled only if the field is provided from the ACS in the PARes message (as specified in the protocol spec). The value should then be passed to the Visa authorization infrastructure as such.

Note the following recommendations:

- Firstly check mdStatus to determine the final status of the transaction.

- The protocol specification requires passing the eci field as such to the authorization infrastructure if it is provided in the PARes message (2.x ARes or PReq). Modirum MPI has value in eci field only if it has been provided in the PARes message (2.x ARes or PReq).

Based on the current understanding of the Visa infrastructure business rules (note that this information is not necessarily accurate and needs to be checked with Visa), the following eci values are recommended to be used in authorization infrastructure:

- 6 = Non-participation and attempts (issuer liability)
- 9x = Service unavailable or system errors (transaction can proceed with the TLS/SSL-secured liability rules, merchant has the liability)
- No value, if authentication or signature check fails

Copyright © 2006-2017 Modirum Ltd, 2017-2018 by VPOS Ltd.
The document may not be published or disclosed to a third party without the written permission of VPOS Ltd.

Fully Authenticated Transactions

In fully authenticated transactions, the issuer and cardholder are participating in the 3-D Secure protocol, cardholder authentication has been successful and signature has been validated.
Scenarios:

- Valid PARes or CPRS message has been received with status Y and the signature has been validated successfully. Or in 2.x ARes or PReq has transStatus Y.

Values:

- mdStatus = 1
- MPI ECI is copied as such from the PARes or 2.x ARes or PReq (often 05 for Visa and 01 for MasterCard)
- Visa authorization ECI value 5 (note that this must be verified from Visa)

Non-participation and Not Enrolled Transactions

In the case, where the card issuer or cardholder is not participating to the 3-D Secure, the transaction can still be completed. Business rules of this case depend on the card scheme. Also, the MPI may determine the non-participation based on the card range missing from the cache.
Scenarios:

- VERes message has been received with status N (there is no difference with the issuer not participating compared with the cardholder not participating).
- MPI uses cache and cannot find the card range in the cache.

Values:

- mdStatus = 2 if card not participating, or mdStatus = 3 if range not in cache
- MPI ECI is empty
- Visa authorization ECI value 6 (note that this must be verified from Visa)

Attempts

In 3-D Secure version 1.0.2, an attempt functionality was introduced. ACS implementations may produce signed attempt-messages even in the cases where the issuer or cardholder is not participating.
Scenarios:

- ACS has produced PARes with A status and signature validation has been successful (can be issuer specific ACS or centralized attempt-server). In 2.x in case ARes or PReq transStatus is A.

Values:

- mdStatus = 4
- MPI ECI is copied as such from the PARes

Authentication Errors

If authentication is not successful, the transaction should not be continued in those cases where the failure is fatal.
Scenarios:

- ACS has provided PARes with status N (e.g too many false passwords or signature check has failed)
- PARes signature validation has failed.
- In case of 2.x ARes or PReq transStatus is N, R

Values:

- mdStatus = 0
- MPI ECI is empty
- Visa authorization ECI value is not relevant, because transaction cannot be continued (note that this must be verified from Visa)

Copyright © 2006-2017 Modirum Ltd, 2017-2018 by VPOS Ltd.
The document may not be published or disclosed to a third party without the written permission of VPOS Ltd.

Authentication Unavailable

In some cases, the authentication may not be available. The unavailable status may come from the directory server or ACS or it may be related to some data communication problems.
Scenarios:

- Directory server produces VERes message with U status or 2.x ARes or PReq transStatus is U.
- Directory server produces VERes or ACS PARes message with U status (e.g mobile protocol not supported)
- No connection to the directory server

Values:

- mdStatus = 5
- MPI ECI is empty
- Visa authorization ECI value 7 (note that this must be verified from Visa)

3-D Secure Errors

3-D Secure related error situations are managed separately.
Scenarios:

- Invalid input field in 3-D Secure message generation
- Merchant authentication in directory server fails
- Error message received from DS or ACS

Values:

- mdStatus = 6
- MPI ECI is empty
- Visa authorization ECI value 7 (note that this must be verified from Visa)

Merchant data errors

If merchant request was invalid or incomplete then:
Values:

- mdStatus = 94
- MPI ECI is empty
- Visa authorization ECI value 7 (note that this must be verified from Visa)

System, networks or directory errors

Sometimes Modirum MPI may produce some error messages related to MPI internal errors. In most cases, it is still recommendable to proceed with the transaction if risk is small.
Scenarios:

- File system full or system misconfigurations
- Database connection lost
- Directory connection fails or response times out

Values:

- mdStatus = 99, mdStatus = 92 or mdStatus = 93
- MPI ECI is empty
- Visa authorization ECI value 7 (note that this must be verified from Visa)

Copyright © 2006-2017 Modirum Ltd, 2017-2018 by VPOS Ltd.
The document may not be published or disclosed to a third party without the written permission of VPOS Ltd.

Fraud Score Block

If Modirum MPI is configured to use a fraud scoring service, the score is calculated prior to attempting 3-D Secure authentication. If the score returned exceeds the allowable threshold, then the transaction is not submitted for authentication.
Scenario:

- Fraud score received from scoring service exceeds configured threshold Values:
- mdStatus = 8
- MPI ECI is empty
- Visa authorization ECI value is not relevant, because transaction cannot be continued with Visa infrastructure (note that this must be verified from Visa)

Pending Transactions

If MPI has passed the PAReq or 2.x CReq to the ACS, the browser session has also moved away from the MPI. Sometimes, the control may never come back to the MPI, which means that there will be a pending transaction in the database.
Modirum MPI does not include a timer to react to the pending transactions, but this functionality needs to be implemented at the merchant site.

The background direct post feature in MPI Server can be used to avoid using the user browser for redirection in return. (This wont help any if user does not return from ACS)
The control flow using background direct post feature is:

1. ACS Posts the PARes (2.x CRes) back to MPI Server via the user browser using the redirection
2. MPI Server determines the status of the transaction and post the status values to merchant payment page using a background session directly from MPI Server to the Merchant payment page server.
3. Merchant server continues with authorization and after the authorization displays the confirmation page to the session opened by the Merchant Server. The Merchant Server passes the page unchanged to the user browser as a response page to the post in step 1.

Summary

The following table summarizes the end status scenarios of the Modirum MPI. The description of ECI values should be placed into the authorization message in the case of Visa.
MPI provides ECI value only if it receives it from the ACS. If merchant receives the ECI from the MPI, that is the value that should be placed in the authorization message. If the ECI value received from the merchant is empty, the merchant should fill out the value prior to sending the authorization message. The suggested values are listed in Visa ECI column. Since these values are Visa region specific, please verify the rules with your local Visa representative. MasterCard uses only ECI values 0 and 1.

Explanation	Log	mdStatus	Eci returned	Visa ECI	Other notes
Authenticated					
Fully authenticated transaction	green	1	From PARes/ ARes/PReq	Use MPI value	CAVV provided
Non-participation					
Issuer or cardholder not enrolled	green	2	empty	6	VERes with N,
Not in cache	green	3	empty	6	Deprecated functionality. Not used.
Authentication Attempt					
Attempt receipt received and signature valid	green	4	From PARes/ ARes/PReq	Use MPI value	CAVV provided
Authentication Unavailable					
Authentication unavailable	red	5	empty	7	VERes or PARes status normally “U”

Copyright © 2006-2017 Modirum Ltd, 2017-2018 by VPOS Ltd.
The document may not be published or disclosed to a third party without the written permission of VPOS Ltd.

3-D Secure Error	red	6	empty	7	Invalid field in 3-D Secure message generation, Error message received or directory server fails to validate the merchant
Network error	red	91	empty	7	If connection to directory times out
Directory error	red	92	empty	7	Directory response read timeout or other failure
Configuration errors	red	93	empty	7	Service disabled, invalid configuration directory deleted before processing ended etc
Input error	red	94	empty	7	Merchant request had errors
Error no directory	red	95	empty	7	No directory server found configured for PAN/card type
Error no version 2 directory	red	96	empty	7	No version2 directory server found configured for PAN/card type and flow requires version 2 processing
System error	red	99	empty	7	
Authentication Not Attempted					
Fraud Score blocked	red	8	empty		No Visa or MasterCard processing
Authentication Failed					
Authentication failed	red	0	empty	Not allowed	PARes status normally “N”
Pares Signature not valid	red	0	empty	Not allowed	
Pending					
Pending transaction	yellow	9			
Perform 3DS method and continue to authentication		50			XML API Only: Perform 3DS method in user browser and sent referencing continue enrollment request after. (fill xid txid in from resp)

Table 5 descriptions

One example of the merchant implementation is as follows:

- Process transactions normally for mdStatus 1, 2, 3 and 4
- Process transactions for mdStatus 5,6, and 9x, if risk manageable
- Never process transactions for mdStatus 0 and 8

Copyright © 2006-2017 Modirum Ltd, 2017-2018 by VPOS Ltd.
The document may not be published or disclosed to a third party without the written permission of VPOS Ltd.

3 XML Interface

Another way to add 3-D Secure support to existing Merchant site is to use XML interface of the Modirum MPI. XSD schema describing message format is located here mdpaympi.war/ModirumMPI.xsd or here http(s)://address/mdpaympi/ModirumMPI.xsd

The control flow using XML interface is the following ThreeDSecure 1.0:

1. Merchant payment page asks the user all the relevant payment data, such as card number, expiry, etc.
2. Merchant payment page calculates digest of Message element (V3.0 or older) to be posted to MDpay MPI utilizing the shared secret or the digital signature (v4.0), sets the digest/signature to ModirumMPI message and posts the ModirumMPI XML to Modirum MPI with Content-Type=application/xml. Note that Merchant should set termUrl parameter in the request message. It should represent Merchant page url, where ACS will post PARes message after user authentication.
3. Modirum MPI checks the card participation from the 3-D Secure directory and if card is enrolled returns the ACS redirection page to Merchant.
4. Merchant redirects user browser using redirection template. After the ACS is finished with the user authentication, ACS returns the control to the Merchant. Merchant receives PARes and sends PAResValidationRequest to the MPI. Message digest should also be uncluded.
5. The MPI Server verifies the signature of PARes and responds to Merchant.
6. Based on returned parameters Merchant proceeds with transaction authorization or stops the transaction in case of error or authentication failure.

The control flow using XML interface is the following ThreeDSecure 2.x browser based:

1. Merchant payment page asks the user all the relevant payment data, such as card number, expiry, etc.
2. Merchant payment page calculates signature of Message element to be posted to MDpay MPI , sets the signature to ModirumMPI message and posts the ModirumMPI XML to Modirum MPI with Content-Type=application/xml. Note that Merchant should set termUrl parameter in the request message. It should represent Merchant page url, where ACS will post (via user browser) PARes or CRes message after user authentication.
3. Modirum MPI checks the card participation from the 3-D Secure directory published ranges and if range is participating 3DS method then
   a) If range participates in 3DS Method merchant is returned EnrollmentResponse with mdStatus=50 (perform 3DS method and continue with enrollment request)
   Merchant shall take html content from field TDSMethodContent and render user a intermediate page where this content is placed into a invisible iframe and wait about 2..3 seconds (or until 3DSMethod completion but not longer than 5 seconds the merchant supplied threeDSMethodNotificationURL is notified if merchant used TDS2.threeDSMethodNotificationURL in intial request then send new EnrollmentRequest filling in only **txId, xid** and TDS2.threeDSCompInd attribute if merchant used TDS2.threeDSMethodNotificationURL on its own.
   b) If range does not participate in 3DS Method then continues to step 4
4. MPI returns
   a) if no errors and challenge was requested then with response message with fild RedirectToACSForm filled with content to be sent to user browser. So user browser posts CReq to ACS for authentication.
   b) With error or final authentication results. Based on results merchant determines if to proceed authorization or not.

   5. After ACS is finished with the user authentication, ACS returns the control to the Merchant. Merchant receives CRes to termUrl (set in initial request) and sends PAResValidationRequest with CRes field filled with CRes content received to the MPI.
   The MPI Server verifies the CRes and matches it with appropriate PReq from directory and responds to Merchant
   with final outcome.
   6. Based on returned parameters Merchant proceeds with transaction authorization or stops the transaction in case of error or authentication failure..

Copyright © 2006-2017 Modirum Ltd, 2017-2018 by VPOS Ltd.
The document may not be published or disclosed to a third party without the written permission of VPOS Ltd.

3.1 XML Parameters to be posted to MPI Server

The following table describes the XML parameters to be posted from the payment page to Modirum MPI. Interface version has been upgraded to 4.0 which utilizes a signature element instead of a digest. The software still supports 3.0, 2.0, but it is not recommended to use versions before 3.0.

Parameters	Type	Required / Optional	Description
ModirumMPI	Root element	R	
Message	element	R	
version	attribute, xsi:string	R	Version of MDpay MPI protocol. Allowed values , 2.0, 3.0 and 4.0 (only 4.0 has been documented in this section).
messageId	attribute, xsi:string	R	Unique alphanumeric message identifier for debugging purposes
md	attribute, xsi:string	R	The MD (“Merchant Data”) field: merchant state data that must be returned to the merchant. The content of this field is passed unchanged and without assumptions about its content to the return Message. This field is used to accommodate the different ways merchant systems handle session state. If the merchant system can associate the final post with the original shopping session without any further assistance, the MD field may be empty. If the merchant system does not maintain state for a given shopping session, the MD can carry whatever data the merchant needs to continue the session. This field must contain only ASCII characters in the range 0x20 to 0x7E; **Since version 4.0.2.15 characters '<' and '>' are not allowed in this parameter.** If other data is needed, the field must be Base64 encoded. The size of the field (after Base64 encoding, if applicable) is limited to 254 bytes. If MD includes confidential data (such as the PAN), it must be encrypted.
merchantId	attribute, xsi:string	R	ID to identify the merchant to MDpay MPI.
lang	attribute, xsi:string	O	Message attribute to specify context language (ISO 639-1 language code en, fi, sv, el, etc..)
RequestMessage	element	R/O	either RequestMessage or ResponseMessage should be present
EnrollmentRequest	element	R/O	either EnrollmentRequest or PAResValidationRequest should be present
Parameters	element	R	
cardType	xsi:string	O	Card scheme can be defined explicitly. Values with 1..2 digits are valid. The value is matched to directory server entry that is mapped to the merchant with that particular cardType The field can also be left empty, which means that the schema/directory server is determined from the card number (see Directory profile settings, cardtypes.xml for card type mappings, and merchant settings in mpimngr to map merchants with particular DS/Acquirer based on card type).
pan	xsi:string	R	Card number. 13-19 digit account number. The value may be: • the account number on the card
expiry	xsi:string	R	Expiration Date supplied to the merchant by cardholder (YYMM). Note that this field is not checked in most of the production ACS installations.

Copyright © 2006-2017 Modirum Ltd, 2017-2018 by VPOS Ltd.
The document may not be published or disclosed to a third party without the written permission of VPOS Ltd.

deviceCategory	xsi:string	O	Integer length 1, Indicates the type of cardholder device. Supported values are:0 = www, 1 = mobile, 4 dtv. Most cases this value shall be allways 0 as wap phones are no longer mainstream and may not be supported by ACSes. Default value is 0
purchAmount	xsi:string	R	Max. 12-digit numeric amount in minor units of currency with all punctuation removed. Examples: Display Amount USD 123.45 Purchase Amount 12345
exponent	xsi:string	R	Exponent number length 1 The minor units of currency specified in ISO 4217. For example, US Dollars has a value of 2; Japanese Yen has a value of 0.
description	xsi:string	O	Purchase description. Brief description of items purchased, determined by the merchant. Maximum size is 125 characters, but merchant should consider the characteristics of the cardholder's device when creating the field. Note: Most Issuers do not display the description to the user.
currency	xsi:string	R	Currency Determined by merchant. ISO 4217, 3 digit numeric.
merchantName	xsi:string	O	**Length**: 1-25 characters **Format**: any characters Send this parameter if you want to override PAReq.Merchant.name. By default it is taken from mpi database
xid	xsi:string	R	Unique transaction identifier determined by merchant. Contains a 20 byte statistically unique value that has been Base64 encoded, giving a 28 byte result.
recurFreq	xsi:string	O	Recurring frequency for PAReq Purchase.Recur.frequency (integer days, 28 means monthly)
recurEnd	xsi:string	O/R	Recurring end date for PAReq format YYYYMMDD, If recurFreq is present then recurEnd is required
installments	xsi:string	O	Number of Installments for PAReq.Purchase.install integer value >1 and <=999. I**nstall and recurring parameters can not be present at the same time.**
termUrl	xsi:string	R	URL of the merchant that MPI will insert as termUrl in ACS redirection template. As a result after cardholder authentication ACS will return PARes/CRes to Merchant instead of MPI.
panMode	xsi:string	O	Possible values: **MDESToken** – to indicate that instead of real pan pan parameter will contain MasterCard Digital Enablement Service Token

Copyright © 2006-2017 Modirum Ltd, 2017-2018 by VPOS Ltd.
The document may not be published or disclosed to a third party without the written permission of VPOS Ltd.

TDS2Attributes	element		3DS 2 related attributes.
Attribute	Element [0..n]		<Attribute name=”aname”>Value</Attribute> Valid attribute names: **Browser based only:** TDS2_BrowserIP TDS2_Navigator_language TDS2_Navigator_javaEnabled TDS2_Navigator_jsEnabled TDS2_Screen_colorDepth TDS2_Screen_height TDS2_Screen_width TDS2_TimezoneOffset TDS2_UserAgent TDS2_BrowserAccept **SDK App only** TDS2.sdkTransID TDS2.sdkReferenceNumber TDS2.sdkAppID TDS2.sdkEncData TDS2.sdkMaxTimeout TDS2.deviceRenderOptionsIF TDS2.deviceRenderOptionsUI TDS2.sdkEphemPubKey **3DS 2.x general extra fields** TDS2.acctID TDS2.acctType TDS2.addrMatch TDS2.cardholderInfo TDS2.cardholderName TDS2.email TDS2.homePhone TDS2.mobilePhone TDS2.workPhone TDS2.messageCategory TDS2.purchaseDate TDS2.transType TDS2.threeDSRequestor3RIInd TDS2.threeDSRequestorAuthenticationInd Since 4.0.2.54 TDS2.threeDSRequestorChallengeInd TDS2.threeDSRequestorID Since 4.0.2.54 TDS2.threeDSRequestorName Since 4.0.2.54 TDS2.threeDSRequestorNPAInd TDS2.threeDSRequestorURL TDS2.challengeWindowSize TDS2.payTokenInd Since 4.0.2.54 TDS2.acquirerBIN Since 4.0.2.54 TDS2.acquirerMerchantId Since 4.0.2.54 TDS2.merchantName Since 4.0.2.54 TDS2.mcc Since 4.0.2.54 TDS2.merchantCountryCode Since 4.0.2.54 **3DS 2.x Merchant Risk fields** TDS2.mriShipIndicator TDS2.mriDeliveryTimeframe TDS2.mriDeliveryEmailAddress TDS2.mriReorderItemsInd TDS2.mriPreOrderPurchaseInd TDS2.mriPreOrderDate TDS2.mriGiftCardAmount TDS2.mriGiftCardCurr TDS2.mriGiftCardCount **3DS 2.x extra account info fields** TDS2.chAccAgeInd TDS2.chAccDate

Copyright © 2006-2017 Modirum Ltd, 2017-2018 by VPOS Ltd.
The document may not be published or disclosed to a third party without the written permission of VPOS Ltd.

			TDS2.chAccChangeInd TDS2.chAccChange TDS2.chAccPwChangeInd
			TDS2.chAccPwChange TDS2.nbPurchaseAccount TDS2.provisionAttemptsDay TDS2.txnActivityDay TDS2.txnActivityYear TDS2.shipAddressUsageInd TDS2.shipAddressUsage TDS2.shipNameIndicator TDS2.paymentAccInd TDS2.paymentAccAge TDS2.suspiciousAccActivity **3DS 2.x extra billing address fields** TDS2.billAddrCity TDS2.billAddrCountry TDS2.billAddrLine1 TDS2.billAddrLine2 TDS2.billAddrLine3 TDS2.billAddrPostCode TDS2.billAddrState **3DS 2.x extra shipping addres fields** TDS2.shipAddrCity TDS2.shipAddrCountry TDS2.shipAddrLine1 TDS2.shipAddrLine2 TDS2.shipAddrLine3 TDS2.shipAddrPostCode TDS2.shipAddrState **3DS 2.x extra authentication info** Information about how the 3DS Requestor authenticated he cardholder before or during the transaction. TDS2.AIAuthMethod TDS2.AIAuthTimestamp TDS2.AIAuthData **3DS 2.x extra authentication info** Information about how the 3DS Requestor authenticated the cardholder as part of a previous 3DS transaction. TDS2.PAIRef TDS2.PAIAuthMethod TDS2.PAIAuthTimestamp TDS2.PAIAuthData See formats in redirection section or emvco spec **3DS 2.x other** TDS2.threeDSMethodNotificationURL – optional send only if You want to detect 3DS method completion on Your pages, else set by mpi. Request to url shall be capable update to TDS2.threeDSCompInd to Y for transaction in question. Since 4.0.2.54 TDS2.threeDSCompInd – **Required in continue to enrollment if** TDS2.threeDSMethodNotificationURL was set by merchant in initial request, else determined by MPI. Since 4.0.2.54 TDS2.broadInfo – JSON object optional Since 4.0.2.54 **3DS 2.x message extensions** TDS2.ME.{N}.name TDS2.ME.{N}.id TDS2.ME.{N}.criticalityIndicator true/false TDS2.ME.{N}.data – JSON object

Copyright © 2006-2017 Modirum Ltd, 2017-2018 by VPOS Ltd.
The document may not be published or disclosed to a third party without the written permission of VPOS Ltd.

Extensions	element	O	
BrazilMarket	element	O	Fill as required by extension specification
Mcc	xsi:string	R	Required if Brazil extension is used. Merchant Category Code, provided by the merchant (Length – 1-4, Numeric digits)
Accounttype	xsi:string	R	Required if Brazil extension is used. Account Type (as selected by the cardholder during checkout) (Length – 1-2, Numeric digits) Code Definitions 00 NOT APPLICABLE 01 CREDIT 02 DEBIT 03 VISA VALE REFEIÇÃO 04 VISA VALE ALIMENTAÇÃO
Mobilenumber	xsi:string	R	Required if Brazil extension is used. Mobile Number (as entered by the cardholder during checkout) (Length – 1-25, Numeric digits)
Transactiontype	xsi:string	R	Required if Brazil extension is used. Transaction Type, provided by the merchant (Length – 1-2; Numeric Digit) Code Definitions 00 Goods / Service Purchase 03 Check Acceptance 10 Account Funding 11 Quasi-Cash Transaction 28 Prepaid Activation & Load
TrustedThirdParty	element	O	
RiskDeterminationTransactionID	xsi:string	O	Required if extension is used, to be filled as specified by extension
RiskDeterminationScore	xsi:string	O	Required if extension is used, to be filled as specified by extension
RiskDeterminationScoreMin	xsi:string	O	Required if extension is used, to be filled as specified by extension
RiskDeterminationScoreMax	xsi:string	O	Required if extension is used, to be filled as specified by extension
RiskDeterminationRecommendation	xsi:string	O	Required if extension is used, to be filled as specified by extension
RiskDeterminationProviderID	xsi:string	O	Required if extension is used, to be filled as specified by extension
RiskDeterminationProviderName	xsi:string	O	Required if extension is used, to be filled as specified by extension
WalletProviderID	xsi:string	O	Required if extension is used, to be filled as specified by extension
WalletProviderName	xsi:string	O	Required if extension is used, to be filled as specified by extension
WalletTransactionTrustLevel	xsi:string	O	Required if extension is used, to be filled as specified by extension
WalletCardholderVerificationStatus	xsi:string	O	Required if extension is used, to be filled as specified by extension
WalletDeviceTrustLevel	xsi:string	O	Required if extension is used, to be filled as specified by extension
WalletSessionTrustLevel	xsi:string	O	Required if extension is used, to be filled as specified by extension
WalletTransactionRefNumber	xsi:string	O	Required if extension is used, to be filled as specified by extension
WalletUserProfileID	xsi:string	O	Required if extension is used, to be filled as specified by extension
WalletLoginMethodStrength	xsi:string	O	Required if extension is used, to be filled as specified by extension

Copyright © 2006-2017 Modirum Ltd, 2017-2018 by VPOS Ltd.
The document may not be published or disclosed to a third party without the written permission of VPOS Ltd.

WalletUserAccountAge	xsi:string	O	Required if extension is used, to be filled as specified by extension
WalletAccountTrustLevelValue	xsi:string	O	Required if extension is used, to be filled as specified by extension
WalletAccountTrustLevelMin	xsi:string	O	Required if extension is used, to be filled as specified by extension
WalletAccountTrustLevelMax	xsi:string	O	Required if extension is used, to be filled as specified by extension
WalletPaymentCardAge	xsi:string	O	Required if extension is used, to be filled as specified by extension
SafeKey EA			
amountTransaction	Xvarnum10 (see XSD Schema)	O/R	Required when extension is present. 1-10 digits,numeric
currencyCode	Xnum3 (see XSD Schema)	O/R	Required when extension is present. 3 digits (ISO 4217 3-digit numeric code)
sellerType	Xnum2	O/R	Required when extension is present. 2 digit numeric value
cmBillingFirstName	Xstring99	O/R	Required when extension is present.. 1-99 character alphanumeric value
cmBillingMiddleName	Xstring99	O/R	Required when extension is present. 1-99 character alphanumeric value
cmBillingLastName	Xstring99	O/R	Required when extension is present. 1-99 character alphanumeric value
cmBillingPostalCode	Xzip	O	5-20 digit numeric value
cmBillingAddress	Xstring99	O	1-99 character alphanumeric value
cmBillingCity	Xstring99	O	1-99 character alphanumeric value
cmBillingState	Xstring99	O	2-99 character alphanumeric value
cmBillingCountryCode	X3166	O	3 digit ISO 3166 numeric value
registeredEmail	Xemail99	O/R	Required when extension is present. 6-99 valid email alphanumeric value
registeredPhone	Xphone20	O	10-20 digit numeric value
registeredPhoneCountryCode	XphoneCC2	O	2 digit numeric value
countOfShipToAddressesOnFile	Xvarnum2	O	1-2 digit numeric value
cmShippingFirstName	Xstring99	O	1-99 character alphanumeric value
cmShippingMiddleName	Xstring99	O	1-99 character alphanumeric value
cmShippingLastName	Xstring99	O	1-99 character alphanumeric value
cmShippingPostalCode	Xzip	O/R	Required if extension is present and shipping method is not electronic delivery (05). 5-20 digit numeric value
cmShippingAddress	Xstring99	O/R	equired if extension is present and shipping method is not electronic delivery (05). 1-99 character alphanumeric value
cmShippingCity	Xstring99	O	1-99 character alphanumeric value
cmShippingState	Xstring99	O	2-99 character alphanumeric value
cmShippingCountryCode	X3166	O	3 digit ISO 3166 numeric value
shippingMethod	Xnum2	O/R	Required when extension is present and transaction is retail. 2 digit numeric value as detailed by the extension
shippingTenure	Xnum8	O	8 digit numeric value
electronicDeliveryEmail	Xemail99	O	6-99 character valid email address
CartItems	Element containing a sequence of cartItem elements	O	
cartItem	Element[1..many]	O	Element with empty body
sku	Attribute.Type: Xstring20	O	1-20 character alphanumeric value
desc	Attribute.Type: Xstring99	O	1-99 character alphanumeric value
price	Attribute.Xvarnum10	O	1-10 digit numeric value
category	Attribute.Xvarnum4	O	4 digit numeric value
qty	Attribute.Xvarnum4	O	1-4 digit numeric value
attributes	Attribute.Xstring99	O	1-99 character alphanumeric value

Copyright © 2006-2017 Modirum Ltd, 2017-2018 by VPOS Ltd.
The document may not be published or disclosed to a third party without the written permission of VPOS Ltd.

IACTransaction	Element	O/R	Element to add SafeKey U.S. market extension data for online travel transactions.
departureDate	Element.xsi:DateTime	O/R	Required when sellerType =01 and transaction amount is equal to $200 or more
Passengers	Element consisting of sequence of passenger elements	O/R	
passenger	Element	O/R	Element with empty body
firstname	Attribute	O/R	1-99 character alphanumeric value
lastname	Attribute	O/R	1-99 character alphanumeric value
origin	Element. Type Xap	O/R	Required when sellerType =01 and transaction amount is equal to $200 or more. 3-5 digit alphanumeric value
dest	Element. Type Xap	O/R	Required when sellerType =01 and transaction amount is equal to $200 or more. 3-5 digit alphanumeric value
airlineCarriers	Element.Type Xstring40	O	1-40 character alphanumeric value
numberOfPassengers	Element. Type Xvarunum5	O	1-5 digit numeric value
PAResValidationRequest	element	O/R	either EnrollmentRequest or PAResValidationRequest should be present. This element is sent to MPI during pares validation step.
pares	xsi:string	O/R	pares message, that is returned from ACS should be passed to this parameter as is. Either pares or c64s should be present.
c64s	xsi:string	O/R	c64s message, that can be returned from ACS should be passed to this parameter as is. Either pares or c64s should be present
ds:Signature	ds:SignatureType	O	The xml signature as defined https://www.w3.org/TR/xmldsig-core/ Canonicalization http://www.w3.org/TR/2001/REC-xml-c14n-20010315 SignatureMethod Algorithm="http://www.w3.org/2001/04/xmldsig-more#rsa-sha256" DigestMethod Algorithm="http://www.w3.org/2001/04/xmlenc#sha256" Requests are signed by merchant private key and validated with merchant Certificate **If missing or mismatching, error is displayed and the request is not further processed.**

Table 6 XML request parameters

3.2 Calculation of the Signature

Signatures shall be calculated and verified according to documentation https://www.w3.org/TR/xmldsig-core/
Canonicalization method to be used is http://www.w3.org/TR/2001/REC-xml-c14n-20010315
SignatureMethod Algorithm="http://www.w3.org/2001/04/xmldsig-more#rsa-sha256"
DigestMethod Algorithm="http://www.w3.org/2001/04/xmlenc#sha256"
The signed element is Message element referenced with its **ID** attribute named **messageId**.
ID attribute is an attribute which type in schema is defined as xsd:ID.

Messages sent by the merchant will be signed by the merchants private key and verified by the MPI using the merchants certificate.

Note that the XML documents should be handled with namespace aware xml libraries (parser/serializer). When the Message element is serialized and canonicalized it should also contain xmlns namespace attribute. See from next section XML message with digest example. Canonitalized message starts for example as:

```
<Message xmlns="http://www.modirum.com/schemas/mpiapi"
md="C62C2F592F1BCA32A24EA877CFF7A461" merchantId="0000001" messageId="M1523010167533"
version="4.0">...
```

Copyright © 2006-2017 Modirum Ltd, 2017-2018 by VPOS Ltd.
The document may not be published or disclosed to a third party without the written permission of VPOS Ltd.

Example code for java:

```
  public static byte[] sign(ModirumMPI root, Marshaller m, DocumentBuilderFactory dbf, PrivateKey
prik, java.security.cert.X509Certificate[] crts) throws Exception
 {
   org.apache.xml.security.Init.init();
   org.w3c.dom.Document document = dbf.newDocumentBuilder().newDocument();
   m.marshal(root, document);// apis.normalizeDOM(dom); dom nomralization is very slow uing instead
msg.setIdAttribute("messageId", true);
   Element modirumMPI = document.getDocumentElement();
   org.apache.xml.security.signature.XMLSignature xmlsigAp =new XMLSignature(document,
null,"http://www.w3.org/2001/04/xmldsig-more#rsa-sha256", "http://www.w3.org/TR/2001/REC-xml-c14n-
20010315");
   Element sigel = xmlsigAp.getElement();
   modirumMPI.appendChild(sigel);
   Element msg = (Element)modirumMPI.getFirstChild();
   msg.setIdAttribute("messageId", true); // setting id attribute instead of dom normalization
   xmlsigAp.addDocument("#" + msg.getAttribute("messageId"),
   null, "http://www.w3.org/2001/04/xmlenc#sha256", null, null);
   for(int i = 0; crts != null && i < crts.length; i++)
   {
    xmlsigAp.addKeyInfo(crts[i]);
   }
   xmlsigAp.sign(prik);
   ByteArrayOutputStream bos = new ByteArrayOutputStream(4096);
   TransformerFactory transfac = TransformerFactory.newInstance();
   Transformer trans = transfac.newTransformer();
   trans.setOutputProperty(OutputKeys.OMIT_XML_DECLARATION, "no");
   trans.setOutputProperty(OutputKeys.INDENT, "no");
   trans.setOutputProperty(OutputKeys.ENCODING, "utf-8");
   DOMSource source = new DOMSource(document);
   trans.transform(source, new StreamResult(bos));
   return bos.toByteArray();
 }
```

Notes: Never calculate signature in user browser using javascript or other script. Or You will expose Your private key to the world. Before passing data to SHA-256 RSA signature function ensure string data is converted to bytes using UTF-8 character encoding.

Example request may look like:

```
<?xml version="1.0" encoding="UTF-8" standalone="yes"?><ModirumMPI
xmlns="http://www.modirum.com/schemas">
<Message version="3.0" messageId="1415803798514" merchantId="sys1331720664552"
md="BAE6B79DBAC72A9019DC36FCC05EEBEC">
 <Request>
  <EnrollmentRequest>
   <Parameters>
    <cardType></cardType>
    <pan>4016000000002</pan>
    <expiry>1812</expiry>
    <deviceCategory>0</deviceCategory>
    <purchAmount>1100</purchAmount>
    <exponent>2</exponent>
    <description>DVD Movies</description>
    <currency>840</currency>
    <xid>7wCBmL39quzo9YMNNipQTAXD9Kg=</xid>
    <recurFreq></recurFreq>
    <recurEnd></recurEnd>
    <installments></installments>

<termUrl>http://localhost:8750/coffeehouse/MerchantHandler2;jsessionid=BAE6B79DBAC72A9019DC36FCC05EE
BEC
    </termUrl>
   </Parameters>
  </EnrollmentRequest>
```

Copyright © 2006-2017 Modirum Ltd, 2017-2018 by VPOS Ltd.
The document may not be published or disclosed to a third party without the written permission of VPOS Ltd.

```
</Request>
</Message>
<ds:Signature>….</ds:Signature>
</ModirumMPI>
```

Example code for Java users to calculate signature:
TODO

Example for .Net users:
TODO

Signatures should be calculated and checked during any communication with MPI be it request or response.

3.3 XML parameters to be returned to Merchant

Parameters	Type	Required / Optional	Description
ModirumMPI	element	R	
ds:Signature	ds:SignatureType xmlns:ds="http://www.w3.org/2000/09/xmldsig#"	O	The xml signature as defined https://www.w3.org/TR/xmldsig-core/ Canonicalization http://www.w3.org/TR/2001/REC-xml-c14n-20010315 SignatureMethod Algorithm="http://www.w3.org/2001/04/xmldsig-more#rsa-sha256” DigestMethod Algorithm="http://www.w3.org/2001/04/xmlenc#sha256"
Message	element	R	
version	attribute, xsi:string	R	Version of MDpay MPI protocol. Allowed values 1.0, 2.0 and 3.0 (only 3.0 has been documented in this section).
messageId	attribute, xsi:string	R	Unique alphanumeric message identifier for debugging purposes
md	attribute, xsi:string	R	The MD (“Merchant Data”) field: merchant state data that must be returned to the merchant. The content of this field is passed unchanged and without assumptions about its content to the return Message. This field is used to accommodate the different ways merchant systems handle session state. If the merchant system can associate the final post with the original shopping session without any further assistance, the MD field may be empty. If the merchant system does not maintain state for a given shopping session, the MD can carry whatever data the merchant needs to continue the session. This field must contain only ASCII characters in the range 0x20 to 0x7E; **Since version 4.0.2.15 characters '<' and '>' are not allowed in this parameter.** If other data is needed, the field must be Base64 encoded. The size of the field (after Base64 encoding, if applicable) is limited to 254 bytes. If MD includes confidential data (such as the PAN), it must be encrypted.
merchantId	attribute, xsi:string	R	ID to identify the merchant to MDpay MPI.
lang	attribute, xsi:string	O	Message attribute to specify context language (ISO 639-1 language code en, fi, sv, el, etc..)
ResponseMessage	element	O/R	either RequestMessage or ResponseMessage should be present
Parameters	element	R	
xid	xsi:string	R	xid parameter from request message

Copyright © 2006-2017 Modirum Ltd, 2017-2018 by VPOS Ltd.
The document may not be published or disclosed to a third party without the written permission of VPOS Ltd.

mdStatus	xsi:string	R	End status of the transaction mdStatus field provides all the information that is needed to determine how to manage the transaction in the merchant system. See section 2.6 Modirum MPI Transaction mdStatus
mdErrorMsg	xsi:string	R	Up to 128 bytes alphanumeric description of the error.
enrollmenStatus	xsi:string	O	The actual value of veres enrollement status like "Y", "N", "U" or "-" if value is not available due errors etc. (since 4.0.2.31). In case of 3DS 2 can have value C as well.
authenticationStatus	xsi:string	O	The actual value of PARes or RReq tx status "Y", "N", "U", "A" or "-" if value is not available due errors or not enrolled. (since 4.0.2.31)
qeci	xsi:string	O	Electronic Commerce Indicator With Visa cards, the value to be passed in Authorization Message (exactly 2 decimal digits). ECI fields determine the final status of the transaction See section 2.6 Modirum MPI Transaction mdStatus
cavv	xsi:string	O	Cardholder Authentication Verification Value Determined by ACS. Contains a 20 byte value that has been Base64 encoded, giving a 28 byte result. Some Visa regions may require that this value be included in the VIP authorization message.
cavvAlgorithm	xsi:string	O	A positive integer indicating the algorithm used to generate the Cardholder Authentication Verification Value. Current defined values are: 0 = HMAC (as per SET™ TransStain) 1 = CVV 2 = CVV with ATN 3 = MasterCard AAV Note that the value is copied directly from the PARes message.
PAResVerified	xsi:string	O	If signature validation of the return message is successful, the value is true. If PARes message is not received or signature validation fails, the value is false. (Compliance testing facility requirement). If signature validation is omitted the value will be empty
PAResSyntaxOK	xsi:string	O	If PARes validation is syntactically correct, the value is true. Otherwise value is false. (Compliance testing facility requirement)
iReqCode	xsi:string	O	Two digit numeric code provided by ACS indicating data that is formatted correctly, but which invalidates the request. This element is included when business processing cannot be performed for some reason. Never provided if mdStatus=0. 3-D Secure iReqCode field.
iReqDetail	xsi:string	O	May identify the specific data elements that caused the Invalid Request Code (so never supplied if Invalid Request Code is omitted). See Table 20 on page 60 for details.
vendorCode	xsi:string	O	Error message describing iReqDetail error.
txId	xsi:long	O	MPI internal transaction id if available
protocol	xsi:string	O	Authentication protocol used in processing. Such as 3DS1.0.2, 3DS2.1.0 or SP5 (Since 4.0.2.54)
cardType	xsi:string	O	Same value as in request or value resolved by MPI. (Since 4.0.2.54)
redirectToACSForm	xsi:string	O	ACS redirection form, containing all the required parameters to be posted to ACS or SecurePlus. PAReq, termUrl, MD and ACS url itself. Form should be presented to user as is. MPI does not set this parameter in response to PAResValidationRequest step.

Table 7 XML response parameters

Copyright © 2006-2017 Modirum Ltd, 2017-2018 by VPOS Ltd.
The document may not be published or disclosed to a third party without the written permission of VPOS Ltd.

3.4 XML interface example

Initial request to MPI:

```
<ModirumMPI xmlns="http://www.modirum.com/schemas/mpiapi" xml
ns:ns2="http://www.w3.org/2000/09/xmldsig#">
<Message md="k5C0IuwfsDK9yubdQYJnh/ck8GHJYI7pEZbSVkk1MoA=" merchantId="0000001"
messageId="MPIER1222501-0" timeStamp="2017-05-17T09:47:58.997+03:00" version="4.0">
  <Request>
    <EnrollmentRequest>
      <Parameters>
        <cardType>1</cardType>
        <pan>##############</pan>
        <expiry>1801</expiry>
        <deviceCategory>0</deviceCategory>
        <purchAmount>000000000112</purchAmount>
        <exponent>2</exponent>
        <description>Order O170517094737</description>
        <currency>978</currency>
<termUrl>https://vposadmin.modirum.com/vpos/PaymentHandler?acsResult=k5C0IuwfsDK9yubdQYJnh
%2Fck8GHJYI7pEZbSVkk1Mo
          A%3D</termUrl>
        <TDS2Attributes>
          <Attribute name="TDS2_BrowserIP">88.196.25.166</Attribute>
          <Attribute name="TDS2_Navigator_language">en-US</Attribute>
          <
              Attribute name="TDS2_Navigator_javaEnabled">false
          </Attribute>
          <Attribute name="TDS2_Navigator_jsEnabled">true</Attribute>
          <Attribute name="TDS2_Screen_colorDepth">24</Attribute>
          <Attribute name="TDS2_Screen_height">1200</Attribute>
          <Attribute name="TDS2_Screen_width">1920</Attribute>
          <Attribute name="TDS2_TimezoneOffset">-180</Attribute>
          <Attribute name="TDS2_UserAgent">Mozilla/5.0 (Windows NT 6.1; Win64; x64) AppleWebKit/537.36
(KHTML, like Gecko) Chrome/58.0.3029.96 Safari/537.36
          </Attribute>
        </TDS2Attributes>
        <xid>MjUwMS1PMTcwNTE3MDk0NzM3LTA=</xid>
      </Parameters>
    </EnrollmentRequest>
  </Request>
</Message>
<ds:Signature xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
  <ds:SignedInfo>
    <ds:CanonicalizationMethod Algorithm="http://www.w3.org/TR/2001/REC-xml-c14n-20010315" />
    <ds:SignatureMethod Algorithm="http://www.w3.org/2001/04/xmldsig-more#rsa-sha256" />
    <ds:Reference URI="#MPIER1222501-0">
      <ds:DigestMethod Algorithm="http://www.w3.org/2001/04/xmlenc#sha256" />
      <ds:DigestValue>g6ckv8JZ8lGbpEuEDLGbPntKLBjzP+QcyjEMwTy9EmY=</ds:DigestValue>
    </ds:Reference>
  </ds:SignedInfo>
  <ds:SignatureValue>
    Ef4cfgN+vvfSt/8ewDdYirqYsyVuGM/ooZCJIpKFYf/wRA1/vXKvJRmfjNgHxMDYitCeNquSX3j5
    TNk5cO7ZxGOQS9IJKPLORCzTIHXWBD0MH16UZnbU08mnfhR+lJzd6kX6qnel+eVrypUaYMviQutG
    mzKAm31AuC4DUEqA9PKRQXdXvGsW5I76sJcTawpNZh7oZf8aK/D1N+FQOUCC+KmtNl5VdgSwuQj9
    Frtz2oGG9nlc/xFtZssJ2gg5/1wLFh4kQkFP3Pg/v5dSOCDzv3PjySS3rR3kKIopU7t7eyQ6muC3
    cjQvJyUZW81u4HEEONWxBzNmTkWajOv4EnQjw6OkcMIvi5UGoQkZcgBAhI0BeyEz9hBgDfFXuSS6
    GSMM2WHbBQh1utnUJEZLfXkPpQvZ3pzzThnYj5v0/hP9aHc=
  </ds:SignatureValue>
  <ds:KeyInfo>
    <ds:X509Data>
```

Copyright © 2006-2017 Modirum Ltd, 2017-2018 by VPOS Ltd.
The document may not be published or disclosed to a third party without the written permission of VPOS Ltd.

```
      <ds:X509Certificate>
MIID5TCCAo0CBFjeXq8wDQYJKoZIhvcNAQELBQAwdzEoMCYGA1UEAxMfVlBPUyBERU1PIHZwb3Nh
ZG1pbi5tb2RpcnVtLmNvbTENMAsGA1UECxMEVlBPUzEQMA4GA1UEChMHTW9kaXJ1bTEQMA4GA1UE
BxMHVGFsbGlubjELMAkGA1UECBMCSE0xCzAJBgNVBAYTAkVFMB4XDTE3MDMzMTEzNTAzOVoXDTIy
MDkyMTEzNTAzOVowdzEoMCYGA1UEAxMfVlBPUyBERU1PIHZwb3NhZG1pbi5tb2RpcnVtLmNvbTEN
MAsGA1UECxMEVlBPUzEQMA4GA1UEChMHTW9kaXJ1bTEQMA4GA1UEBxMHVGFsbGlubjELMAkGA1U
E
CBMCSE0xCzAJBgNVBAYTAkVFMIIBYjANBgkqhkiG9w0BAQEFAAOCAU8AMIIBSgKCAUEAyhFCdFGD
      pchDXC7ryDUiMOlRHjce4N9e4hNUZ6+hTshRBTNeHqcTfhxKuiReaC6AVbQEbBYBGCUs8EQAWppK
      RIB+ZnTytY8bhJqQ1YuiWvAN5cTBLoS2jE5vxf/Xx/+G+UhjfmK6XM0UKnQ4mR+MKM5/iSgV/Un7
      ysHoLLepwefEUBQEODqAIsc6N5pMeeShT/66WEtxEkiXQPn48PXDRLLzSBzB247w03r+92WWrlVe
      IMgTQc0kgx2gsgMziiqiUDSB69Bm/ugT81wDcUNklmbo8r3IsxtjOT+/HQ8Qbo4vQpJI7yzIcnvt
      6U8Ub5TLjz4UmIBg8y6lY/kbJoxA/4n/M+1MwZqgM7cKGi5lG429A3h/1g2zhQ8bZBexnY5FLW1G
PTCS4ahE67ZYl8CWXjoDAzFtVcdpMDFnvZ6noMkCAwEAATANBgkqhkiG9w0BAQsFAAOCAUEAp0mN
      /2Ml6tVC8Zi0bkXJ8j+bUxaxCUU1nV7htzWOqlAsQn1mVb7lbkLZgOc7RfD5CxdLspAVIVU1Gekp
      /tSLjbdA3obSlBFmIm5yU4PGN9YjLRi5jbAAJNhJYThFB0YJu4M6tqX0nbxX6GphPeh2ruQ6WzeS
      KwUf62gqd96WZeIwAKLoAZng4G9LZNITL7jUgl4OWq9OzZ+JYpe/rSz1tKWAg9r5U/AEkoZasfPo
      3MLQlNCTh/WQm8jmtsyglct4k5SNI3ABhFcPfcR0PIhCjTVd7vlY8NcdaxSYYRzQgKZ7N8pdhvi3
      NyPZmbu4OJXkc4Fupuyp2YxhGh0AtLKvdPRmybNZCmTRejgGbJeE6LjkcJ2zcunb+LxbyoxJ1DdU
      K1tddzVPdH+QK8q3EKBNt0H3KwbRPk9qRmH4xuoX4XA=
      </ds:X509Certificate>
    </ds:X509Data>
  </ds:KeyInfo>
</ds:Signature>
</ModirumMPI>
```

MPI response with ACS redirect template:

```
<?xml version="1.0" encoding="utf-8" standalone="no"?>
<ModirumMPI xmlns="http://www.modirum.com/schemas/mpiapi"
xmlns:ns2="http://www.w3.org/2000/09/xmldsig#">
<Message md="k5C0IuwfsDK9yubdQYJnh/ck8GHJYI7pEZbSVkk1MoA=" merchantId="0000001"
messageId="MPIER1222501-0" version="4.0">
  <Response>
    <Parameters>
      <xid>MjUwMS1PMTcwNTE3MDk0NzM3LTA=</xid>
      <mdStatus>9</mdStatus>
      <mdErrorMsg>To be redirected to acs</mdErrorMsg>
      <enrollmenStatus>Y</enrollmenStatus>
    </Parameters>
    <redirectToACSForm>&lt;!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01//EN"
"http://www.w3.org/TR/html4/strict.dtd"&gt;
      &lt;html&gt;
      &lt;head&gt;
      &lt;title&gt;MDpay default response template for web&lt;/title&gt;
      &lt;script type="text/javascript"
      language="javascript"&gt;
      function moveWindow() {
      var form = document.getElementById("downloadForm");
      if (form != null) {
      form.submit();
      }
      }
      &lt;/script&gt;
      &lt;/head&gt;
      &lt;body&gt;
      &lt;form id="downloadForm"
      action="https://3ds-acs.test.modirum.com/mdpayacs/pareq"
      method="POST"&gt;
      &lt;input type="hidden"
      name="PaReq"
```

Copyright © 2006-2017 Modirum Ltd, 2017-2018 by VPOS Ltd.
The document may not be published or disclosed to a third party without the written permission of VPOS Ltd.

value="eJxVUttuwjAM/ZWKp+2lSXrLikwkBkhDWgFx+YAqNWu39ULarrCvX1LK2PLkc07s2MeBfaoQ5zuUrUIB
EdZ1/IZWlkxGYeBTXo0EbKZbPAn4QlVnZSGYTW0HyA3qHCXTuGgExPL0vFwJrz9ABgg5quVcMMf1/ADIFUE
R5yhm5fGImJZtjdZDgnn5CKQXQJZt0aiLcFwXyA1Aqz5F2jTVmJCu6+y8TDLV5rYscyBGA3JvZtOaqNa1zlkiovd
DF+3YJtrLbrVfuNH8g66+I/d1P50AMTcgiRsUDmWc+oxbNBh7fOyHQHoe4tw0IRaHrcVspucfCKjMO9MrYEb4S4
C2VWEhLyLkT3qQGwI8V2WB+oZO+I0hwVqKtUpQWetrHzT0uMt1E0YBch9q9mL8lo320nG5EzicGcd7wlTPtF/s
ibK+vAFATAoZlkmGTevo3w/4AW3urPk=">
<input type="hidden"
name="TermUrl"
value="https://vposadmin.modirum.com/vpos/PaymentHandler?acsResult=k5C0IuwfsDK9yubdQYJnh
%2Fck8GHJYI7pEZbSVkk1MoA%3D">
<input
type="hidden"
name="MD"
value="k5C0IuwfsDK9yubdQYJnh/ck8GHJYI7pEZbSVkk1MoA=">
<!-- To support javascript unaware/disabled browsers
-->
<div style="text-align: center;">

<noscript>
<center>Please click the
submit button below.
<input type="submit" name="submit" value="Submit"></center>
</noscript>
</div>
</form>

<script type="text/javascript">
moveWindow();
</script>
</body>
</html></redirectToACSForm>
</Response>
</Message>
<ds:Signature xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
<ds:SignedInfo>
<ds:CanonicalizationMethod Algorithm="http://www.w3.org/TR/2001/REC-xml-c14n-20010315" />
<ds:SignatureMethod Algorithm="http://www.w3.org/2001/04/xmldsig-more#rsa-sha256" />
<ds:Reference URI="#MPIER1222501-0">
<ds:DigestMethod Algorithm="http://www.w3.org/2001/04/xmlenc#sha256" />
<ds:DigestValue>gNJwiQO3qpKAHybkru+31B1Y8V9haD8Q0mfFwu2eo/k=</ds:DigestValue>
</ds:Reference>
</ds:SignedInfo>
<ds:SignatureValue>
PzQiFtORzYRqB9wk0PBe2Ki0tvg9R2S5YVK95BKsK9hdRrUc+uNGXbvcEY+POtcTAj8zQPkf8Ztn
rUB81kWsNhBvLSytfZslmxYXS/XM7gvYOPINa0kOcqT0e/F7egq4M7ZhYxFM6SebmlKkXPySATfv
qZCoaNJh0DUTxB9l/PvAjr1UISv5K2xmm9XqZd75oE6Zf+QFFWppNhaDBGUiFHw9iG1VqwFw9nqI
sfw8kIpu8kIhqp4zu3oibXaLgVcqcpXNf8PQixFafuTHGhzbb/R3hd2sTUMSrt/M5PQmhufKi++O
FIV34mRBmkit5KCrovEE/ACO9vBgG6w5RJUabzLJkhkOv5TZwufzxX12OxWVcXQRKcwzsNNBzhaz
gPG7tMPkfBhIDXdeQPliKghGvRqpCWuPX9mqc1lbHoucdgM=
</ds:SignatureValue>
<ds:KeyInfo>
<ds:X509Data>
<ds:X509Certificate>
MIID5TCCAo0CBFjeXq8wDQYJKoZIhvcNAQELBQAwdzEoMCYGA1UEAxMfVlBPUyBERU1PIHZwb3Nh
ZG1pbi5tb2RpcnVtLmNvbTENMAsGA1UECxMEVlBPUzEQMA4GA1UEChMHTW9kaXJ1bTEQMA4GA1UE
BxMHVGFsbGlubjELMAkGA1UECBMCSE0xCzAJBgNVBAYTAkVFMB4XDTE3MDMzMTEzNTAzOVoXDTIy
MDkyMTEzNTAzOVowdzEoMCYGA1UEAxMfVlBPUyBERU1PIHZwb3NhZG1pbi5tb2RpcnVtLmNvbTEN
MAsGA1UECxMEVlBPUzEQMA4GA1UEChMHTW9kaXJ1bTEQMA4GA1UEBxMHVGFsbGlubjELMAkGA1U
E
CBMCSE0xCzAJBgNVBAYTAkVFMIIBYjANBgkqhkiG9w0BAQEFAAOCAU8AMIIBSgKCAUEAyhFCdFGD

Copyright © 2006-2017 Modirum Ltd, 2017-2018 by VPOS Ltd.
The document may not be published or disclosed to a third party without the written permission of VPOS Ltd.

```
        pchDXC7ryDUiMOlRHjce4N9e4hNUZ6+hTshRBTNeHqcTfhxKuiReaC6AVbQEbBYBGCUs8EQAWppK
        RIB+ZnTytY8bhJqQ1YuiWvAN5cTBLoS2jE5vxf/Xx/+G+UhjfmK6XM0UKnQ4mR+MKM5/iSgV/Un7
        ysHoLLepwefEUBQEODqAIsc6N5pMeeShT/66WEtxEkiXQPn48PXDRLLzSBzB247w03r+92WWrlVe
        IMgTQc0kgx2gsgMziiqiUDSB69Bm/ugT81wDcUNklmbo8r3IsxtjOT+/HQ8Qbo4vQpJI7yzIcnvt
        6U8Ub5TLjz4UmIBg8y6lY/kbJoxA/4n/M+1MwZqgM7cKGi5lG429A3h/1g2zhQ8bZBexnY5FLW1G
PTCS4ahE67ZYl8CWXjoDAzFtVcdpMDFnvZ6noMkCAwEAATANBgkqhkiG9w0BAQsFAAOCAUEAp0mN
        /2Ml6tVC8Zi0bkXJ8j+bUxaxCUU1nV7htzWOqlAsQn1mVb7lbkLZgOc7RfD5CxdLspAVIVU1Gekp
        /tSLjbdA3obSlBFmIm5yU4PGN9YjLRi5jbAAJNhJYThFB0YJu4M6tqX0nbxX6GphPeh2ruQ6WzeS
        KwUf62gqd96WZeIwAKLoAZng4G9LZNITL7jUgl4OWq9OzZ+JYpe/rSz1tKWAg9r5U/AEkoZasfPo
        3MLQlNCTh/WQm8jmtsyglct4k5SNI3ABhFcPfcR0PIhCjTVd7vlY8NcdaxSYYRzQgKZ7N8pdhvi3
        NyPZmbu4OJXkc4Fupuyp2YxhGh0AtLKvdPRmybNZCmTRejgGbJeE6LjkcJ2zcunb+LxbyoxJ1DdU
        K1tddzVPdH+QK8q3EKBNt0H3KwbRPk9qRmH4xuoX4XA=
      </ds:X509Certificate>
    </ds:X509Data>
  </ds:KeyInfo>
</ds:Signature>
</ModirumMPI>
```


PARes validation request to MPI:


```
<ModirumMPI xmlns="http://www.modirum.com/schemas/mpiapi"
xmlns:ns2="http://www.w3.org/2000/09/xmldsig#">
<Message md="StndCjQrZpcH8XTvAmFrGX2bm9wZrmYszyiym7k1OhA=" merchantId="0000001"
messageId="MPIPVR1222501-0" timeStamp="2017-05-17T09:48:04.825+03:00"
     version="4.0">
  <Request>
    <PAResValidationRequest>
      <pares>eJzVmFmzoziy

gP9KRc2jo5vFYEOH60SIHRsw+/bGZsBsZjPLr7/4nDrVNXVrImbu01xeQImUSilTX0o6mVmXJIyRRGOXvJ3kpO
+DNPmSx9++kgccPj6+vp1UoCf9u6jCYXh/ILBN+Ey6Pm/qN+RP

+E/0BH0WNw1dlAX18HYKopYSlTfs/TlB34unKulE5g1B9xh+OEEfpRP0dzN1fH31mzFzHr/Jd2uSDUSVzWhSTH
YvMwWsrPJeMsG3E/SqcYqDIXlDYeQI48jxC3z4Czv+hZMn6F1+erzUgaoZN90Isln6s+C0jbpL6mh5I4/ECfpROiXz
o6mTrcbW4Mf3CfrbtkdQv8E/PS/Fm+hkum+nIa9+MYj4C95m4F1+6odgGPs37wR9/zpFwfP5BgCgAGvnkQZezz2q
zjP4eLaBvlc5JVH+BuObRdv7vRUo06bLh6x62fnPghP0MgV6993bycjTeuusS77MVVn3375mw/D4C4Kmafpz2v/Zd
CmEbqOAYBLaKsR9nv7j60erJBbrW/N2ooO6qfMoKPM1GDZPy8mQNfGXHx3+TqWpv7QikM7Sf2xq/4gQrP7jJY
H3CL7ph36v9Cdz/51efjW864M/+ixAXh38oujtpCe35OXj5Iuli9+
+/uOniGbyNOmH/0uPn739rOFTnx2UY/KmHO86xdmOGR0tCh93cRu3eCz7+sP69tnuo+YJ+mHid/s/PfBjLB8VOb
XVKudZuZDaSqRGmwtFV1JW2QrGt70+ItWyjnFjie5dX8hDdmtYGl4jgqBTCrFFs88a5qa7VpDrhVjQO70NGaCyh
SXvnYzecbay1I3VtxU4C01jHW4wk6y+1LcPGSdJFBWqXEEKyXBFEkPEi3LdCxEEhUsIHrqCN+4lVc9UOnScPJP
1XQ2lupECujU4U6B3kd9cqUshac+
+suPL+cldtfti393lAKKzP/UhI8cYN1iszEQ1G4yNquqhoaMXgm+OoxUKbkRIVZM93GAAFUwEs9e6Ek72ECLWm
T5J2HTtafrMyTabPzs5I32hOrNLpsDXobaFdl8/WtzHOWa0IFyvGYuvlmUG3779FDTfPXJJlg8PuDhMMsEQfHzRS
Tfkty16N8zIosh4Jk2DokrBJFIgFW0gOYPFObDtS8uEl+hdqhSsH+ZFilEZwDxttLwhhntGYyl6soDMpzOzAoVKFZs
CskmV1NnmSEYzWVumZB4gFkvPsmwXZ8fm7TXmFCRw9VLW4ImePMbWtAs76Y5hK5SsEROjvcsEdvJZ38FR
3xVn1gTqh/7UpFnlGfLk4jn6U9b6if6oz7PT2bZWkHATPCsrWOS7vL3FWV714CW7mv8sk/lppldw/tDrmaDAVVn3
Jg582oQoIao/otoeRBZhI57DZcOaxA+bJXaet1lQYN/RUgu1l7gq774rpzZrmzaNmDbLCYaFC7KOTcKHToadbcd3zw
+/KkufpvLEoN7HLXKKqJnilKZs/uscA80CABMpZgKv/xfQbH7SGL5p0TguBT4Elzqa8YfKlnqamSVf9fnTTPfuET
M1hiY5c9DwdV4lVqDXHuwqeqFdjdPlp1YItNy06e4iJnmjS8eAdaDiIMe54Xt4ZNqhWwRlSDPwBEUaM8ddU5N6
X2M4gOeiDnOPaJOhQuV74lFlKTsOcRQmEV4iF4XOY1QPI40oR+TJq8V4OBJOXVRX1tdDMuWFJJCqcYrRPLv
nj2A4qq1MDSxRr3oEwuvTii4mw18P03Mf4Y26Q3nVjoalQqllJrs5tMkZHRIxiCW0EWmF3t9jNUbPS3HMEBWnt
WC4QehonjMQ7EjseeDIm8CCUb0RrXrzrpN59OfDZVHHCcpLGR0FqAa4CVKZAoB9xeD50vhi9owUoLESpQFm
m/vt316rZCGKpPoAQfq+cpxwrYopWG2+VS3Ar+1FyGdiCkPzEj728TZdZ7Edi+k4HCTK2o+D4VHHOn1ER7wXj
GKBeGI09zck3e+kgl9kskbdDn48n8d7CjwNLGfwODYBNG7hwdO3WXMs7gLlC1lecSLrYdFl25iAgo1VDMryzAF
BL6EaOfTxnA96lxWjrygXOxsPWC+kF1TYyJgr9NxeGN6MwYzP03NwDUdj0pY4DFLad9KQIcqiRzaBnMmBTR
bjAIioMYUwZEtG6jqexcyCzGiOnCIksZ/ikwuv0A1L9wTZprLuKyVDHUJulnbdjYi6xuFs0VLqBz0QubiDWqzHlI0
mHi0r5RZv0QavX8n0O1Sx/AtVE/
+JKh1IXkS6uHYcjNk85PyOrfLKtn7nvikwWUkGxTuOqEymbVueGRNIH8u/MSnOf0QoO0srGD5kvXku32Wp4eD
wtmxHz9UfIYpnIU2ZWxkNHKUUWW6NUPIeOBwcOOQo683E/1junBO4Siby9j1EkWFrc/cNStfM75i6A1w2i0Vm
5FVh4hemlg1ds2yyk8LI2Ev234XXbf4N8df5pb4vDxUw23+tod+XyqWLfUiz7hPGrMWx4PDa9I9Xr60K5LhPsfCZ
```


Copyright © 2006-2017 Modirum Ltd, 2017-2018 by VPOS Ltd.
The document may not be published or disclosed to a third party without the written permission of VPOS Ltd.

YvruImDIOqzRZI2Kemi6fuf3EQoZnH6bUPkmT8h1UlFFrrOMbIiYyuzjuUlYy47I6a7AjnBgdkMLhPAOG0F7zdqMI
kaoDEqDnIXw8VwKiMVX/s6b16m5g1l0H0VCjMYBNUdcuFwofn5mPnQ2wXiLqae0z3eW3N4KxZxdb2PtJYaF/C
AI3fNalO3EEjumFx/Y6ncPj4H0MWawThP4yTU0OCAoZdbWpWqce5Nfe9kWvUuKPEtN9CcS6xTSrsNBb+AY6co
+egC2OSiFGlOox1eMI/rHaQoPPcccNa7hz7FJuHlBCdHAHFQ/IeJ6/xj6Lf5ZAIIr9WRoajSB8fKboG/YuhEszQAeaA
IEUhbIgvaKjVgE+iDz/RRoHudjLLP5a4sKcKfStKNSlqO0iAa65waCDkdMs01BvI8XHH3F7Zb5n6FBTgFaTFfNEy
+Tt/naEra1N20nGY/LOMN3qd57rQNOb4JX+uNtLGYAs9lA8f/6//Xdbo14t3uL6y1uvEl4xZoOXynKYzm5SZMC3H
2OisQULMXNMKDzNtQz1f1uG/JKkUCju57JARrtnK5CzB1r4rAS8yTKFAyfFxck79eWnjQB85InHt8n2KaeR5KOj
WXoZCvNoAhOIG9FqgeDrFdRUZPcbnCjLhHqvoyFrB3YBi1dfZ9yqNDQq+r1jYI27mBMfERsudsaClEXU8RHC
WkvVo0tHCM1MnNHz7qOAM0oWtOu5NJHvzQubgnCA5bNasXY0T0oPf3YLYA5n7191+M0uJtLKXuavj/3B8B05
jFdrpNwQ4dnLl3qAaENQVh2OH1YMCK4srdzUx1NcE2x8l4Whc5dL4xjWVGJnKlCGJLZkhrI9bddNObqUnJBo4s
fHDL3aJ/nQqHgLUF10BXD8uNzx/tOasr8g7jc2fnfxDN335b/8/CJZy0ZRsSQ50fNKqCuryui7tTBfKGsaLMi58kJfu1
uOMBQj/+NGlaRQf+Bt0xm7apcPZN9yjT8ibzqXWZQ57DWy6jCs5gvn2HF9dtuqoxq/
+GhVqq5yhqiyuMD3djM34H3iVLW/sC772xh7iCbjleYcpRMYS5jsqu8AVy+g1VeI/hqN5tM/lX2X5ZW/gM8K4V1K
y/Vo8bRwRP3/kApqqN6W2q+nGtIsJ2IY3aGnQdXi3Iygk+WeAwVqKEnXhyK22V+Gjmj65Vxoy3xTLWwU7Lafoy
AFELUTrx2+qSled/uQwUWfQlE8CqIj8Vxxypoiv7YB/qT6QN06sIVYgekLWT4DjUC9Lx2W9q7COSZxNuCbrEtbf
RstOD1ZboxxYNDb03hD7B1uXDDbAuRwaoGi6yKgmxRPBvK4/h8uMv8lIyehty4I/ijSadoiCyz63D3ToWRcQtTtj5f
zNoXMRq1kmya7xtN6ZvRmxDgnzOT3Ry169gBHEw6Ysju+iCZx+QquXHm1bWILMu5Cbw1uymZeGlusg2JYtEP
PI8mTQ33j7T6iWfK3LC44fn/PZqpmRCWINaAU2LUSO0tZibXlVMKcf0VzZT2A80JwqOZ2gOw0xulgSO7RnZm
EhGGF2sU4I4tXUskl2TBiB2T/eFm80q+XotFNEkg8E130BFJDLKLu2MPVauZXr/WZwPP3DPBExGswtV8t40oPC
7FpOETtZ2sHRkN3csjl8zEs50bAjrOaR/IQvIHHQbXoJbu1aToFOjS5XkoEc0Pj5a8p26kgZfw2HGyBG+BQlBHsiwT
3N2j4pO838ZoPESB2FFSoRrzwWt37ZZ8e4xQdOOq7CC1rUhhnhBhDy0r2ko8tpricT7bDGv4POtup5aJPrvM4aonL
spB1GDFRIvu47vrh7aXizeWTMJu21AjOEqVNi34KL+o8T0TRykRUMQOTSheWEEAv0Ez9Pd5H/pxB/D37cD7re
X7denrsu3na9T/Af5LBqc=</pares>
    </PAResValidationRequest>
  </Request>
</Message>
<ds:Signature xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
  <ds:SignedInfo>
    <ds:CanonicalizationMethod Algorithm="http://www.w3.org/TR/2001/REC-xml-c14n-20010315" />
    <ds:SignatureMethod Algorithm="http://www.w3.org/2001/04/xmldsig-more#rsa-sha256" />
    <ds:Reference URI="#MPIPVR1222501-0">
      <ds:DigestMethod Algorithm="http://www.w3.org/2001/04/xmlenc#sha256" />
      <ds:DigestValue>+NGJpXUDc2M3+vG8c8hccR081PSAC5aPzWlYcUvDXec=</ds:DigestValue>
    </ds:Reference>
  </ds:SignedInfo>
  <ds:SignatureValue>
    b/NklbvW/pyCeCu+ZLt5rqpUsClVr3gu4EWbYz935rlZpvX/Oq0NssZD5SiH06jT5WZx5Sq9QL7J
    JCySHsa819q5TCxkKaNgQS2+NUw4q2SEAEBHfkJIZ4dDmeJnH4AuebAryQxa3NVW2Lmz4SZfx8MG
    4o7CSBKqueNsJP1u3SMsQl8YEVOptwC23e1yfiPYip6KBDtIibcpk5r/GCHZJw3maWAYZ5YZXjig
    3cVfGroxWuVCBaXKNquZQgy5/uhwBHpFoKBPqiy/CInkSpm1kTtNdkSCNmOzzqqcW3i3DHF44bJq
    UEbpOtSeLRhOxHOHnfzpFaG1+tEcdEXSj5JcffVpg+6YNsGrfCIE2Ays295s6OPWAGQuekcCcUbM
    zLXIVDBvtXo7vqf09v4NBBjqydnyFwvBuZcNWxk64Pp+qRc=
  </ds:SignatureValue>
  <ds:KeyInfo>
    <ds:X509Data>
      <ds:X509Certificate>

MIID5TCCAo0CBFjeXq8wDQYJKoZIhvcNAQELBQAwdzEoMCYGA1UEAxMfVlBPUyBERU1PIHZwb3Nh

ZG1pbi5tb2RpcnVtLmNvbTENMAsGA1UECxMEVlBPUzEQMA4GA1UEChMHTW9kaXJ1bTEQMA4GA1UE

BxMHVGFsbGlubjELMAkGA1UECBMCSE0xCzAJBgNVBAYTAkVFMB4XDTE3MDMzMTEzNTAzOVoXDTIy

MDkyMTEzNTAzOVowdzEoMCYGA1UEAxMfVlBPUyBERU1PIHZwb3NhZG1pbi5tb2RpcnVtLmNvbTEN

MAsGA1UECxMEVlBPUzEQMA4GA1UEChMHTW9kaXJ1bTEQMA4GA1UEBxMHVGFsbGlubjELMAkGA1U
E

CBMCSE0xCzAJBgNVBAYTAkVFMIIBYjANBgkqhkiG9w0BAQEFAAOCAU8AMIIBSgKCAUEAyhFCdFGD
        pchDXC7ryDUiMOlRHjce4N9e4hNUZ6+hTshRBTNeHqcTfhxKuiReaC6AVbQEbBYBGCUs8EQAWppK

Copyright © 2006-2017 Modirum Ltd, 2017-2018 by VPOS Ltd.
The document may not be published or disclosed to a third party without the written permission of VPOS Ltd.

```
        RIB+ZnTytY8bhJqQ1YuiWvAN5cTBLoS2jE5vxf/Xx/+G+UhjfmK6XM0UKnQ4mR+MKM5/iSgV/Un7
        ysHoLLepwefEUBQEODqAIsc6N5pMeeShT/66WEtxEkiXQPn48PXDRLLzSBzB247w03r+92WWrlVe
        IMgTQc0kgx2gsgMziiqiUDSB69Bm/ugT81wDcUNklmbo8r3IsxtjOT+/HQ8Qbo4vQpJI7yzIcnvt
        6U8Ub5TLjz4UmIBg8y6lY/kbJoxA/4n/M+1MwZqgM7cKGi5lG429A3h/1g2zhQ8bZBexnY5FLW1G

PTCS4ahE67ZYl8CWXjoDAzFtVcdpMDFnvZ6noMkCAwEAATANBgkqhkiG9w0BAQsFAAOCAUEAp0mN
        /2Ml6tVC8Zi0bkXJ8j+bUxaxCUU1nV7htzWOqlAsQn1mVb7lbkLZgOc7RfD5CxdLspAVIVU1Gekp
        /tSLjbdA3obSlBFmIm5yU4PGN9YjLRi5jbAAJNhJYThFB0YJu4M6tqX0nbxX6GphPeh2ruQ6WzeS
        KwUf62gqd96WZeIwAKLoAZng4G9LZNITL7jUgl4OWq9OzZ+JYpe/rSz1tKWAg9r5U/AEkoZasfPo
        3MLQlNCTh/WQm8jmtsyglct4k5SNI3ABhFcPfcR0PIhCjTVd7vlY8NcdaxSYYRzQgKZ7N8pdhvi3
        NyPZmbu4OJXkc4Fupuyp2YxhGh0AtLKvdPRmybNZCmTRejgGbJeE6LjkcJ2zcunb+LxbyoxJ1DdU
        K1tddzVPdH+QK8q3EKBNt0H3KwbRPk9qRmH4xuoX4XA=
      </ds:X509Certificate>
    </ds:X509Data>
  </ds:KeyInfo>
</ds:Signature>
</ModirumMPI>
```


PARes validation response from MPI:


```
<?xml version="1.0" encoding="utf-8" standalone="no"?>
<ModirumMPI xmlns="http://www.modirum.com/schemas/mpiapi"
xmlns:ns2="http://www.w3.org/2000/09/xmldsig#">
<Message md="StndCjQrZpcH8XTvAmFrGX2bm9wZrmYszyiym7k1OhA=" merchantId="0000001"
messageId="MPIPVR1222501-0" version="4.0">
  <Response>
    <Parameters>
      <xid>MjUwMS1PMTcwNTE3MDk0NzM3LTA=</xid>
      <mdStatus>1</mdStatus>
      <mdErrorMsg>Authenticated</mdErrorMsg>
      <enrollmenStatus>Y</enrollmenStatus>
      <authenticationStatus>Y</authenticationStatus>
      <eci>05</eci>
      <cavv>AAABAEVicQAAAAAjcmJxAAAAAAA=</cavv>
      <cavvAlgorithm>2</cavvAlgorithm>
      <PAResVerified>true</PAResVerified>
      <PAResSyntaxOK>true</PAResSyntaxOK>
      <txId>96507</txId>
    </Parameters>
  </Response>
</Message>
<ds:Signature xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
  <ds:SignedInfo>
    <ds:CanonicalizationMethod Algorithm="http://www.w3.org/TR/2001/REC-xml-c14n-20010315" />
    <ds:SignatureMethod Algorithm="http://www.w3.org/2001/04/xmldsig-more#rsa-sha256" />
    <ds:Reference URI="#MPIPVR1222501-0">
      <ds:DigestMethod Algorithm="http://www.w3.org/2001/04/xmlenc#sha256" />
      <ds:DigestValue>eXmv0YqTgw3StXqaj/PsvZ6KJAzlb05dzCPPuoieo3c=</ds:DigestValue>
    </ds:Reference>
  </ds:SignedInfo>
  <ds:SignatureValue>
    CdudW1IP7LkYxcl1JQJRt8WwtGgyRC7q+6MuKisOQk/avISLKN9mzu7UsYsrAXQEtx3KwZVVhV/y
    PF4j5qwAHw7+Uib7tfLjO3+vZ8bOgl3I8KVWbXjgsLRbghidqGvMr3ieRO4SKwrDJQ8jQ/7ptjnd
    rmCOwa1hKhSP3FFpwiRUZAVYyGU2Ji32h3VrU4BLp/0lqZF8Kju+P861K36vgeNxt9PTgdyCiTln
    E3yo5kPczop2EvLg92MZ4xBfO995Nv+d5BKCw1kl4GaskEVOG/hRlD5gCS6Ehw4l5yKEwK5Nb2qS
    k/WEMj9A9NQVZv8+MyRxQKTFB/9wPB7yvXP6rRraEvREgTk0VMvZFZPFM/BKsnoN88JBYGQ6UUA0
    py+HAjm1HcRIyyh7BfznkmdWggxEgP0mysscfNYdir02yTM=
  </ds:SignatureValue>
  <ds:KeyInfo>
    <ds:X509Data>
```


Copyright © 2006-2017 Modirum Ltd, 2017-2018 by VPOS Ltd.
The document may not be published or disclosed to a third party without the written permission of VPOS Ltd.

```
      <ds:X509Certificate>

MIID5TCCAo0CBFjeXq8wDQYJKoZIhvcNAQELBQAwdzEoMCYGA1UEAxMfVlBPUyBERU1PIHZwb3Nh

ZG1pbi5tb2RpcnVtLmNvbTENMAsGA1UECxMEVlBPUzEQMA4GA1UEChMHTW9kaXJ1bTEQMA4GA1UE

BxMHVGFsbGlubjELMAkGA1UECBMCSE0xCzAJBgNVBAYTAkVFMB4XDTE3MDMzMTEzNTAzOVoXDTIy

MDkyMTEzNTAzOVowdzEoMCYGA1UEAxMfVlBPUyBERU1PIHZwb3NhZG1pbi5tb2RpcnVtLmNvbTEN

MAsGA1UECxMEVlBPUzEQMA4GA1UEChMHTW9kaXJ1bTEQMA4GA1UEBxMHVGFsbGlubjELMAkGA1U
E

CBMCSE0xCzAJBgNVBAYTAkVFMIIBYjANBgkqhkiG9w0BAQEFAAOCAU8AMIIBSgKCAUEAyhFCdFGD
      pchDXC7ryDUiMOlRHjce4N9e4hNUZ6+hTshRBTNeHqcTfhxKuiReaC6AVbQEbBYBGCUs8EQAWppK
      RIB+ZnTytY8bhJqQ1YuiWvAN5cTBLoS2jE5vxf/Xx/+G+UhjfmK6XM0UKnQ4mR+MKM5/iSgV/Un7
      ysHoLLepwefEUBQEODqAIsc6N5pMeeShT/66WEtxEkiXQPn48PXDRLLzSBzB247w03r+92WWrlVe
      IMgTQc0kgx2gsgMziiqiUDSB69Bm/ugT81wDcUNklmbo8r3IsxtjOT+/HQ8Qbo4vQpJI7yzIcnvt
      6U8Ub5TLjz4UmIBg8y6lY/kbJoxA/4n/M+1MwZqgM7cKGi5lG429A3h/1g2zhQ8bZBexnY5FLW1G

PTCS4ahE67ZYl8CWXjoDAzFtVcdpMDFnvZ6noMkCAwEAATANBgkqhkiG9w0BAQsFAAOCAUEAp0mN
      /2Ml6tVC8Zi0bkXJ8j+bUxaxCUU1nV7htzWOqlAsQn1mVb7lbkLZgOc7RfD5CxdLspAVIVU1Gekp
      /tSLjbdA3obSlBFmIm5yU4PGN9YjLRi5jbAAJNhJYThFB0YJu4M6tqX0nbxX6GphPeh2ruQ6WzeS
      KwUf62gqd96WZeIwAKLoAZng4G9LZNITL7jUgl4OWq9OzZ+JYpe/rSz1tKWAg9r5U/AEkoZasfPo
      3MLQlNCTh/WQm8jmtsyglct4k5SNI3ABhFcPfcR0PIhCjTVd7vlY8NcdaxSYYRzQgKZ7N8pdhvi3
      NyPZmbu4OJXkc4Fupuyp2YxhGh0AtLKvdPRmybNZCmTRejgGbJeE6LjkcJ2zcunb+LxbyoxJ1DdU
      K1tddzVPdH+QK8q3EKBNt0H3KwbRPk9qRmH4xuoX4XA=
    </ds:X509Certificate>
  </ds:X509Data>
 </ds:KeyInfo>
</ds:Signature>
</ModirumMPI>
```


Copyright © 2006-2017 Modirum Ltd, 2017-2018 by VPOS Ltd.
The document may not be published or disclosed to a third party without the written permission of VPOS Ltd.

4 SOAP interface

As of MPI 4.0.2.42 there is an opportunity to send SOAP 1.2 messages to MPI. Interface reflects format and behavior of XML interface. There are a few differences:

1. XML messages should be sent with SOAP envelope. Examples below.
2. Messages should be sent with ContentType=application/soap+xml

WSDL schema is located here mdpaympi.war/ModirumMPI.wsdl or here http(s)://address/mdpaympi/ModirumMPI.wsdl.
Message contents of SOAP are equal to XML API only wrapped to SOAP envelopes.

4.1 SOAP interface example

Initial request to MPI:

```
<?xml version="1.0" encoding="utf-8" standalone="no"?>
<env:Envelope xmlns:env="http://www.w3.org/2003/05/soap-envelope">
  <env:Header/>
  <env:Body>
    <ModirumMPI xmlns="http://www.modirum.com/schemas/mpiapi"
xmlns:ns2="http://www.w3.org/2000/09/xmldsig#">
      <Message md="535CF439C39D63F978C1B58845C2005D" merchantId="sys1331720664552"
messageId="M1494972873437" version="4.0">
        <Request>
          <EnrollmentRequest>
            <Parameters>
              <pan>4016000000002</pan>
              <expiry>1812</expiry>
              <deviceCategory>0</deviceCategory>
              <purchAmount>1100</purchAmount>
              <exponent>2</exponent>
              <description>DVD Movies</description>
              <currency>840</currency>

<termUrl>https://bank1.modirum.com:443/coffeehouse/MerchantHandler2;jsessionid=535CF439C39D63F978C1B58
845C2005D
              </termUrl>
              <xid>VGnMqa+1jNBTSnCnoh3K8PuiVZQ=</xid>
            </Parameters>
          </EnrollmentRequest>
        </Request>
      </Message>
      <ds:Signature xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
        <ds:SignedInfo>
          <ds:CanonicalizationMethod Algorithm="http://www.w3.org/TR/2001/REC-xml-c14n-20010315"/>
          <ds:SignatureMethod Algorithm="http://www.w3.org/2001/04/xmldsig-more#rsa-sha256"/>
          <ds:Reference URI="#M1494972873437">
            <ds:DigestMethod Algorithm="http://www.w3.org/2001/04/xmlenc#sha256"/>
            <ds:DigestValue>ngY4nXCbtb00r8Uwb7ElwhMshoX3a1H/JkonU6yIzqI=</ds:DigestValue>
          </ds:Reference>
        </ds:SignedInfo>

<ds:SignatureValue>AuausHQxQuVWIE7V/ZMoT8PeDSTJhpUTImyPGS+EWOUqMkJMAogZQh/xiM9H+0g9cZ9
fXa9zkdX8j83AK0pnfy768CZU7MZ4kLIn50W/qaf62NNvS2o2BTQSpfnFjz4DX11hcKZzProdY63C/wqJHwOO
bN9al96mKm0kFkqU0batWnCRRnzD8blJZOZ35j+hdI5bTZjnXYsrft3FVhUlb0WbQccVfULmksnR
Ozf/DeKxo0vjvJCLCWYfu4plMrUKT6xCzsALWR8ycx4/kpWi9ICpemVIyOeXGZantH+p/s8RTk0r
+F1iVyTxOVGgmryHGxFizYA79g9ZAHmC0gugrg==
        </ds:SignatureValue>
        <ds:KeyInfo>
          <ds:X509Data>
```

Copyright © 2006-2017 Modirum Ltd, 2017-2018 by VPOS Ltd.
The document may not be published or disclosed to a third party without the written permission of VPOS Ltd.

```
<ds:X509Certificate>MIIERTCCAy2gAwIBAgIJAKcoY+m8gQgZMA0GCSqGSIb3DQEBCwUAMHQxCzAJBgNV
BAYTAkVFMREwDwYDVQQIEwhNeSBTdGF0ZTEQMA4GA1UEBxMHbXkgQ2l0eTEVMBMGA1UEChMMQ2
9tcGFueSBOYW1l
MRAwDgYDVQQLEwc3NzExMjIzMRcwFQYDVQQDEw53d3cubXlzaXRlLmNvbTAeFw0xNzA0MDIxNDE0
MjJaFw0yMTA0MDExNDE0MjJaMHQxCzAJBgNVBAYTAkVFMREwDwYDVQQIEwhNeSBTdGF0ZTEQMA4G
A1UEBxMHbXkgQ2l0eTEVMBMGA1UEChMMQ29tcGFueSBOYW1lMRAwDgYDVQQLEwc3NzExMjIzMRcw
FQYDVQQDEw53d3cubXlzaXRlLmNvbTCCASIwDQYJKoZIhvcNAQEBBQADggEPADCCAQoCggEBAM8d
E9IUNgDgZMHgbvvAeacl7BOk2HROV+ikDN1PK8dW5sz+VBiNXzuBl0sdJzeDaPXMjRwHpXQmI6PM
HIPsVAFQGGChU6FruwLzE8W4dxOyP4QwP1lK0M0bOtsZoQR92SMLzpRSvyTgpxyUt0anl0DeEwqQ
1xywOjDcYo2wDcGh9KHimFu4+ABi+xd3XHo/a0bjG2LAdluMMrr8+0SPzhqQRBz7d9p4icqOnjcG
TGMTKwL/MprFRWtowzo59Vb+BkQZLr6qhQwUy6e7HU5rf8S7ng1b9CE5b/Y/1GytRuZzrIGSSQep
F3a9u3UuJFf6TkiZ/F/DQUgGSNPoo/Hek50CAwEAAaOB2TCB1jAdBgNVHQ4EFgQUM/JziGyZzQAP
Thvn2bvneMGd3Z8wgaYGA1UdIwSBnjCBm4AUM/JziGyZzQAPThvn2bvneMGd3Z+heKR2MHQxCzAJ
BgNVBAYTAkVFMREwDwYDVQQIEwhNeSBTdGF0ZTEQMA4GA1UEBxMHbXkgQ2l0eTEVMBMGA1UECh
MM
Q29tcGFueSBOYW1lMRAwDgYDVQQLEwc3NzExMjIzMRcwFQYDVQQDEw53d3cubXlzaXRlLmNvbYIJ
AKcoY+m8gQgZMAwGA1UdEwQFMAMBAf8wDQYJKoZIhvcNAQELBQADggEBAA7Afh9bQGMrAbmWMzV
d
Sl0mipz7EdNvdHoB8uJ+/VN7+cPCl5Wv3gnBNxbK7pCKoH2ECnAD4o91RT9winoCLaduMCBWIdbV
5AiZbmPSOw52byIZn0MCTPW0dkphQtJdDRxtFFLzZQPLfUBF5xasSveF/JT09p/ukcbkmE6w7TPd
4ivHis0vPJAEooA4oVGBIEJHOkdThu0myX+VsDU1K2JCWQ2IkymJdkxgMOGEUFAHTd8Xo7Z5Guqv
WRA7YrvsR1tclN0FKS0ICbbuUb3nFxx2BboPvGC4H5dUagoVDrmotSChNVUVOLlE+YTI9ojyqMFB
pAhfSIiDh2jcOvPq1F4=
            </ds:X509Certificate>
          </ds:X509Data>
        </ds:KeyInfo>
      </ds:Signature>
    </ModirumMPI>
  </env:Body>
</env:Envelope>
```

MPI response with ACS redirect template:

```
<?xml version="1.0" encoding="utf-8" standalone="no"?>
<env:Envelope xmlns:env="http://www.w3.org/2003/05/soap-envelope">
  <env:Header/>
  <env:Body>
    <ModirumMPI xmlns="http://www.modirum.com/schemas/mpiapi"
xmlns:ns2="http://www.w3.org/2000/09/xmldsig#">
      <Message md="535CF439C39D63F978C1B58845C2005D" merchantId="sys1331720664552"
messageId="M1494972873437" version="4.0">
        <Response>
          <Parameters>
            <xid>VGnMqa+1jNBTSnCnoh3K8PuiVZQ=</xid>
            <mdStatus>9</mdStatus>
            <mdErrorMsg>To be redirected to acs</mdErrorMsg>
            <enrollmenStatus>Y</enrollmenStatus>
          </Parameters>
          <redirectToACSForm>&lt;!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01//EN"
"http://www.w3.org/TR/html4/strict.dtd"&gt;
            &lt;html&gt;
            &lt;head&gt;
            &lt;title&gt;MDpay default response template for web&lt;/title&gt;
            &lt;script type="text/javascript" language="javascript"&gt;
            function moveWindow() {
            var form = document.getElementById("downloadForm");
            if (form != null) {
            form.submit();
            }
            }
            &lt;/script&gt;
```

Copyright © 2006-2017 Modirum Ltd, 2017-2018 by VPOS Ltd.
The document may not be published or disclosed to a third party without the written permission of VPOS Ltd.

</head>
<body>
<form id="downloadForm"
action="https://3ds-acs.test.modirum.com/mdpayacs/pareq"
method="POST">
<input type="hidden"
name="PaReq"

value="eJxVUcluwjAQ/ZWIa6U4TsJSNIwERCqoAtFCOfQWOUOTqrGDnbD8fe2wtT7Ne+PZ3oNNromSNYlGE8
KCjEm/yCuyUYdH3SCqOgir8TvtEQ6kTaEkcj/wQ2A3aGu0yFNZI6RiP5kvMW4fsCuEkvQ8QR5GcbcH7IJApiXhV
O12RDPVGPIyKpVnclUBa3MgVCNrfcYwtlU3AI3+wbyuqyFjx+PRL1VW6Kb0hSqBuRywxz6rxkXG9joVGW5f5
GKfPvHv5WSzllOp8uh1sGqK7efbCJj7AVlaE4YB7wdd3vPCcMjjYRQBa3lIS7cEfqwTj1sRAnvhhYHKDRpfAOcu8
5cBq60mKc44iG3qjoBOlZJkf1g57zFkZAQm28RbqENBxk53BLDHNdOZ01rUVscw6lufnrlTuyVc08IKxQf80tUBY
K6EXY1kV5dt9M/9X/zRraA=">
<input type="hidden"
name="TermUrl"

value="https://bank1.modirum.com:443/coffeehouse/MerchantHandler2;jsessionid=535CF439C39D63F978C1B5884
5C2005D">
<input type="hidden"
name="MD"
value="535CF439C39D63F978C1B58845C2005D">
<!-- To support javascript unaware/disabled browsers -->
<div style="text-align: center;">

<noscript>
<center>Please click the submit button below.
<input type="submit" name="submit" value="Submit"></center>
</noscript>
</div>
</form>
<script type="text/javascript">
moveWindow();
</script>
</body>
</html>
</redirectToACSForm>
</Response>
</Message>
<ds:Signature xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
<ds:SignedInfo>
<ds:CanonicalizationMethod Algorithm="http://www.w3.org/TR/2001/REC-xml-c14n-20010315"/>
<ds:SignatureMethod Algorithm="http://www.w3.org/2001/04/xmldsig-more#rsa-sha256"/>
<ds:Reference URI="#M1494972873437">
<ds:DigestMethod Algorithm="http://www.w3.org/2001/04/xmlenc#sha256"/>
<ds:DigestValue>4ACquN4SO0Dg9DZp7QG2GacukQkwuicEbexzlOKcjrM=</ds:DigestValue>
</ds:Reference>
</ds:SignedInfo>
<ds:SignatureValue>
rXYl+kWPqma87EYT5SLgSMILL56FlVsGrVVKqhDuc91WfwXXf0fNaB3RbPPg0BOflsTDTLo04UJ/
e5VaioL4JOO1reBeg+qglkGmESeFRpSNtpAnOTrRJycvIVoUkc1blmhErBCIiB6CH1CX9aaCtsdk
xalhEBBH0YhC4uUHzVvzmLEvcZIHvxW42Zlq1fWRilTQCkoxADv+MrV9LrTVnrOTX80gNcWe6eFB
Yla1t7fSl2cyD0M7/HtJ5KMKtP2AFwqaJjTkIIIY1n49GU45SJSUqxNKwOXyTmfh9N+qwVlEp0yS
y8Ty3HQ1u/f76EkrDyDPKrrb6jkTjS9mjQc+9A==
</ds:SignatureValue>
<ds:KeyInfo>
<ds:X509Data>
<ds:X509Certificate>
MIIEDDCCAvSgAwIBAgIJAPmMWIp6hdlRMA0GCSqGSIb3DQEBCwUAMGExCzAJBgNVBAYTAkVFMQ4w
DAYDVQQIEwVTVEFURTERMA8GA1UEBxMIbG9jYXRpb24xDDAKBgNVBAoTA29yZzELMAkGA1UECxM

Copyright © 2006-2017 Modirum Ltd, 2017-2018 by VPOS Ltd.
The document may not be published or disclosed to a third party without the written permission of VPOS Ltd.

```
C
T1UxFDASBgNVBAMTC3d3dy5tcGkuY29tMB4XDTE3MDQxMDE0Mjk1NFoXDTIxMDQwOTE0Mjk1NFow
YTELMAkGA1UEBhMCRUUxDjAMBgNVBAgTBVNUQVRFMREwDwYDVQQHEwhsb2NhdGlvbjEMMAoGA
1UE
ChMDb3JnMQswCQYDVQQLEwJPVTEUMBIGA1UEAxMLd3d3Lm1waS5jb20wggEiMA0GCSqGSIb3DQEB
AQUAA4IBDwAwggEKAoIBAQDABIBYhYb1eG3hNhmqaF6+TKd7FVnZZhRKZsRk4gOThpmQgb4JDc3G
o25m1RriU7K/ChRJG10FYfTWVdzhzFUPUljgkTK3Kw3/cxMGJVyBgB+E7MORYN83kZng0nSof+XB
di7jI37GjdY6YbQ2XhvOLHJVHuwVwMXa1oBtoFbH/xrIbZbADWXu/HSbaR646EKaatUZxrHGn+yS
b5cvzkVPJZWftMOv0vZSuJNmuWLjZ1fcibrY6k1Y8IyTBajTrrOv+logS3mNlVsSxRc/923O1Mqc
UlvGwMiTrsc/SFom1jkpkRmj3Tbf2xH+uGPI2sNJ0Y1oKGpjc2e92OGPcBNJAgMBAAGjgcYwgcMw
HQYDVR0OBBYEFKUAYaOMNxyv021FrFM/tQn67CzPMIGTBgNVHSMEgYswgYiAFKUAYaOMNxyv021F
rFM/tQn67CzPoWWkYzBhMQswCQYDVQQGEwJFRTEOMAwGA1UECBMFU1RBVEUxETAPBgNVBAcTCGx
v
Y2F0aW9uMQwwCgYDVQQKEwNvcmcxCzAJBgNVBAsTAk9VMRQwEgYDVQQDEwt3d3cubXBpLmNvbYIJ
APmMWIp6hdlRMAwGA1UdEwQFMAMBAf8wDQYJKoZIhvcNAQELBQADggEBAGjOX36cEik4FDRuyIy9
gMzz36s8EPhEWd+b1RFJEvheOJOgnbrBZbd4OLrzW1JBzZ3qq1XRsFr+tw9zKCIpl6sVxgzKYt4O
Z2LKG1+N1OD9wHE9jZ1dYaRNEsmcurcyX6cRyIvNsT0ioJxNFSMGf5iJGYP+b88Ist5r1xs3rq8V
a2PLQ1rB4S02/U2C6h+iYWyYv95d9+acrwbPpIwvEFRWPUnR2gzgBL/Gs0O0jiNcNyuUR5nJDIUf
Us0ERAYWdRmRlEK7pmxqkhRqsLF2exWpmkK8rBGh5JD8908Nu9aB+efMDB4582J5vcz7VV2zwRKY
orvXz6ca1a62exlyoQw=
            </ds:X509Certificate>
          </ds:X509Data>
        </ds:KeyInfo>
      </ds:Signature>
    </ModirumMPI>
  </env:Body>
</env:Envelope>
```


PARes validation request to MPI:

```
<?xml version="1.0" encoding="utf-8" standalone="no"?>
<env:Envelope xmlns:env="http://www.w3.org/2003/05/soap-envelope">
  <env:Header/>
  <env:Body>
    <ModirumMPI xmlns="http://www.modirum.com/schemas/mpiapi"
xmlns:ns2="http://www.w3.org/2000/09/xmldsig#">
      <Message md="535CF439C39D63F978C1B58845C2005D" merchantId="sys1331720664552"
messageId="M1494972873437" version="4.0">
        <Request>
          <PAResValidationRequest>
            <pares>

eJzVWNmyozqy/ZWK6kfHOQwGG064doSYMQabeXhjMsbM8/D1jfeuXae6um5E3/vUlxejJZFKKVeulHUyHm0c
M3ocDm38dpLjrvOT+EsaffuK7HF4X399O92AFnfvUIGRR5Qg0A0c47ZLq/IN+RP+Ez1Bn83NQhs+/LJ/O/lhQ4nK
G/b+nKDvzVMRtyLzhqB7DD+coI/WCfr7s9vweus2Z+Y0erP4Um78HfJUKEMv6bJ67CXiNqSWp347Qa8Rp8jv4zc
URo4wjhy+oOhfCPbXfn+C3vFT/TIHimrYbCMIDJ+gn5HTtuw2LsPljcC2rh+tUzzXVRlvI7a1/Xg/QX87V/vlG/zTs41
7QSfDeTv1afFvHmHbgHf81PV+P3Rv7gn6/nYK/XF8AwBQgBeRTAWv5xkatgY+nm2l70NOcZi+wfjm0fb7/hXIk6p
N+0fx8vNfgRP0cgV6D97bSU+Tcpusjb/MRV52374+
+r7+C4Kmafpz2v9ZtQmEbquAYBLaBkRdmvzj68dXcSSW9+rtRPtlVaahn6er32+hluP+UUVffkz4O5OG9rKKQBpL/
7GZ/SNEsPKPFwLvEXyzD/3e6E/u/iez/Op42/l/dA8feU3wi6G3kxbf41eM4y+mJn77+o+fKM2kSdz1/5cZP2f72cKnP
cvPh/hNSlpBJRz0emeFcbzXRbuLLzPaP6cXj38eeYJ+uPjd/88I/FjLx8CLFQzy8IS9mbKoaEgoQ8go3tZN5liKMUbeF
XuFGdXmLl19rR2UE4dqcc7s9R7jj+tRjyQrVvnlmE42oVXyuaIob1kE/SD7MzOKBzm631SfahC04fAbZks6fLzGvrt
zKNO5hJbnDKO7nHl06dKDw46lUTXQ7RreojO8HA4Zu7fvJJmRJoy6kDhZGhlxDzkz1wZpQMf0Optpl5xHvWHP
+tj9nnBeUxoT42lZ3681hNl7ad8zDlIvUzpgAnGAzDFhxz1fECOSdZMWa7v2qTTQUATnp19Z1xFyrgpumt4BH5l4v
g9y/TiHgZtRKeCUAKtLFtlvaMxafMsXgpvUSX1uJHJ4emFxqKA2+fbtJ9J8j4gULx8RcHCYZPze/3ij47ZP7xt7N52
RRZFxDZoGWZGASaRAIlrgYvcmZ8OWd1kmPEefl0LBun5eLhEqA5in9YbXxWDPqCxFTyaQ+WRmVqBQiWJR
QDaonDpbHMmoBmvJlMwDxGTpWZat7GxbvLVGnIL4jpbLKjzRk8tYqiqxk2brlkLJKjEx6jsmsJPHejaOeo44swa4f
dhPDJpVxoAnF9fWRlntJvpjPM9OZ8tcQcxN8KysYJGf8vYrzvKq+S/savwrJvPTTK/g/GHXNUCG32TNnTjw6ROi
BKhWh6XViyzChjyHy7o5iR8+X9h53nZBgT1bTUzUWqIif3qOnFisZVg0YlgsJ+gmLsgaNgkfNhl2tmzPOddekeceTa
WxTr2vW+QUUTXEKUnY9Nc9BqoJACZSzARe/RKotjipDF81aBTlAh8AqQxnvL6xuZY8jJwvunQ0kr1zxAyVoUn
```

Copyright © 2006-2017 Modirum Ltd, 2017-2018 by VPOS Ltd.
The document may not be published or disclosed to a third party without the written permission of VPOS Ltd.

O6FV8ndcLK9BrB3YFvdCOymnyqGYCLVdNspPEOK20y9FnbSjbMijVPRcPDStwMj8PaAaeoFBl5qitSlLrSgwH8J
yVQeoSTdwXqPyMXSrPZdsmjsIkwkvooNB5CMt+oBHliIz8LRsOR8Ius+LKelpAJrwQ+5dimCI0fTzT2u+Pt0amep
YoVy0EwXU0Q8lg+OthGvchXt12KH+zwn4pUGqZyXYOLHKToVj0owtaibRC75/RLULPS3Z8IDecVv3+DqGDcX
4Af0di44Ej7wILhtudaG539zoZR28+SMttmKA0l9FBgEqAGyCRKQDYFwfPUuWJjzFUgMpeKBUw295vfXu1kIU
wvJQHCNL2hW0Ha5FN/mrxzc0E/NpIQjoTUxAYUlDvo227zmIzZNOxP1wocz/0uksdy6QOj3gn6NkC8cRg7O9Ist9
dMn6RyRJ1Wrgex+MzAa4KljOoj5UPDRs9ePo+q7bJSVC6kPkVJx4dLDpsExGQT5ZPBmV55oCgUnALbfp4TnutF
WSDpyiS9RgOWCckEip0TZEq9NxIDG9EYMbnaewd3VaZpCEO/SXp2kv/QJRFCy0COZM9Gy/6ARBhZQhBwOb
MpW15FjMy8kFz5BQisTWKIxdcoTuW7AmySWTNU3KGOgTcfNm1dyJsK5uzRFMpa7onUnEHNViHKZuauLSs5
Bvfwk28flWm30kVy7+kauI/pUoDFzckHVw99vpsHFJ+xxZpYZm/C9/kG+xFBtm7HFEPmbYseWYMcPlI/8qgOK8
OUXa+rKD/wDrjnL9jiW7j8Ja2g+todYDij4CmjK2N+raSiyy3hij59G0O9m1ykLVq4n+kO2f7jvIQeesZoEi/ffP0dEpTj
e8y9QS4bGSLzMirwkQvmVo26Zplg50URsZe2H+XvG77r4u/7i/1PT1ugNn61Yp+TxWpjTxINZ8TxqzZMePw0vCO
V7cpMuS4T7BgTDBtJwkYsvZrOJmDcjtUbbfzuhCFdE67T6h8lyfkOt1QRS4fD7IiIuphHc9VzJpWSE5PBbaFA7PrG
yAET1j3m+ujeVDEAOV+rpOzENTjkkEsvvJP3rhO1RPMolNnMTHoB9QYcEGSKH4eHx50NsBwj6jxsk93ptzcM8
WYHXfTWimChfQgCO14zfJmYokd04k1tnpt7TKQNkQM1qoCPzm6CvsEpczquhSV/azSaydboislyJirojeRWKuQVh
n0WgVHSJt3YQ3Y6qBkt4hCXb5gbNE7TlNw6DjmqHIVf44MwkkzSgh75nDzYiIq93XfbfxnAfCv1MjQ1GAA/RU3
Qdtk606wNAN4oAoQSFggC+qLG5EItF7mu8lXXc7DWGaL18YK8KSSpKUSlqPUkAaa6/iCBodMtW1BtI8WHH3
xdqv8Y6CTk49m01V1RWlyt1ibwpZ708UALvfgdM+hOveVB5xW+a/yx1tYxABm84Hi/
+f+67vfKvHu98brjTfuJLy4psFXinJZTq6SOANPj6NCMQFLdtd16Lwt9Uy1vzuGvEokUOm2Y1KAhju7LRBjxxo4r
EQ8iTIZw6eZhKTd2tCTKmBuPOLRc4ItajySdKQvfSubyQMK4RhyV6SoGWS9isotTq0K18scoZ7LkMnqga3Q3NH
2CYcKFb3e3K5S0Mrp9YkPia12m30mamKCeChx2YtFZQnH8BYaqa092pYA1SCa0y7nkrpbKgc3BaGGZaNYMXZ
wDkpH17sFMOezu287nAZPY8llV9X25+4AmNY4Jst1Eu5oP6YXqewRWheEZYfThwUj/Ct7P1fF0QDXBMufeZZp
3FVibNMMc+RMZUIfz+alghwPsUTM0S6xhIaS5x8eztE6z5lCwVuBaqErhqXHccd7dmLIfE1IT3b+D+WZe27pPx4+
5VmN+wHR5Xk7viqgLK8rctvdeuMlZVnzyFKenODX6YYDDFX/u9Swigy6D3l7yKxV5KtrsKNMw5+SV7xjOnUO
Si0PC/wR8fkYFFy3nabysPRqFzUT1VHWAFXqD+nGZv4J3E8pZa0PeffsjeY2stl40ZSjZApzGINd5U3A5SdY5TWE
r1a1YfKv2H9ZWflfyLOSmfdcKuoSR3tX3Hs9pdzsm7uVZulcQoJlhxyz063Uv5qU/SD4eImGQIEqeuLFPrtL86injKY
V+p02xTPVwHbOqvshBJcAonbitdUmNUm7Zh8osOhdQAivglgvtjMUfpV1x87XRqbz0akNVojtkSaT4SdUCdB4bbe
yJwnkmcSbjG6wrWx0bLjgpTTdmazm0HuVeT1sShLXz5YQ6uxNZ5FVUZCNxbOu1MexdpZ5vOgdDTlRS/BHg07
QAFlmx+ae7Q1Gho2mbHmWjNITMRo148c0Pzc1pe96Z0CAH2fmcbdvbcv24GDQIUO215pk6slRUv3M39YsNE37
LvDm7CRk7CapwVYkioU/5HkwaKp/fpTVT3mmjE0WN3n+fy/N1EwIix+pwM4xaqD2JjOT68opmbj+Ks2U+kOaY
4RHH7cOgJ1WKRUcWiWyM+KQ0N1IpQB3bOjyQnLxwx+wY7w/3C1eSddrtogGCQS+ag8achH9h+Ts2EPRqIbbre
VZxx/OmeCJEL7Bxfy09DA4Ltmk4hPlNo4to4Ej1enFiF3LviOg5eymRhaSP2gwuPrl5VlMikaBNlnGQ46oXnA05T11
J3U8h4eWky/wRhSCOpJ5HuPOHhVH8nkfwuEQ+mJLXbKbPh/cZtdsxbfDCEXTr8oOujUFKcwTIuyhZUWbC4+th
niczxbD6h7POtu/lok+O8zhqsUOykFUb0ZEg+6jp+MFlpuKd5aMg3Y7UCM4SuUWLXgov9yi50McLrGAIlZgQNH
CCgL4jTRDf//fh37cAfx9O/B+bfl+X/q6bPv5HvWfn+sHWA==
            </pares>
          </PAResValidationRequest>
        </Request>
      </Message>
      <ds:Signature xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
        <ds:SignedInfo>
          <ds:CanonicalizationMethod Algorithm="http://www.w3.org/TR/2001/REC-xml-c14n-20010315"/>
          <ds:SignatureMethod Algorithm="http://www.w3.org/2001/04/xmldsig-more#rsa-sha256"/>
          <ds:Reference URI="#M1494972873437">
            <ds:DigestMethod Algorithm="http://www.w3.org/2001/04/xmlenc#sha256"/>
            <ds:DigestValue>mOZ4WMPNRTfY/Uj4SWKRNBdKvrt+X7xgPpdxz7PBFMI=</ds:DigestValue>
          </ds:Reference>
        </ds:SignedInfo>

<ds:SignatureValue>lU6U6+SThF1697DBGJ8cEf7kJIH6R9NzVriTtr8Tq9dvbTKDT4BeBGHyTRRbhPiGG05whfR
DAXpy+JwgwhRKRjgScd1uudCpPdkOW0IPvCdT6/BGOEMy+OSBLhUGpoykSb3hS7xyQ2mVuFLJ3MSY8/o6a3
W61IRSnNPvi1ENpqudgAU1Qg8Opy8aHqy6nzquAFnjQlYbrJmB/5UCZkwMpUiK1F6fWz27yY8N1l5hJ/P/bE1SYf
OjUQSQqd1ZXJ4czAY8S1uzrNCbjtcxtoev6/TtUI46mnQmCfEXyxtK3Qfzkff
YWqVdZ+Rxd/ZQ7zL5DD69IUvo2jRzOdO6+n6uw==
        </ds:SignatureValue>
        <ds:KeyInfo>
          <ds:X509Data>

<ds:X509Certificate>MIIERTCCAy2gAwIBAgIJAKcoY+m8gQgZMA0GCSqGSIb3DQEBCwUAMHQxCzAJBgNV
BAYTAkVFMREwDwYDVQQIEwhNeSBTdGF0ZTEQMA4GA1UEBxMHbXkgQ2l0eTEVMBMGA1UEChMMQ2
9tcGFueSBOYW1l

Copyright © 2006-2017 Modirum Ltd, 2017-2018 by VPOS Ltd.
The document may not be published or disclosed to a third party without the written permission of VPOS Ltd.

```
MRAwDgYDVQQLEwc3NzExMjIzMRcwFQYDVQQDEw53d3cubXlzaXRlLmNvbTAeFw0xNzA0MDIxNDE0
MjJaFw0yMTA0MDExNDE0MjJaMHQxCzAJBgNVBAYTAkVFMREwDwYDVQQIEwhNeSBTdGF0ZTEQMA4G
A1UEBxMHbXkgQ2l0eTEVMBMGA1UEChMMQ29tcGFueSBOYW1lMRAwDgYDVQQLEwc3NzExMjIzMRcw
FQYDVQQDEw53d3cubXlzaXRlLmNvbTCCASIwDQYJKoZIhvcNAQEBBQADggEPADCCAQoCggEBAM8d
E9IUNgDgZMHgbvvAeacl7BOk2HROV+ikDN1PK8dW5sz+VBiNXzuBl0sdJzeDaPXMjRwHpXQmI6PM
HIPsVAFQGGChU6FruwLzE8W4dxOyP4QwP1lK0M0bOtsZoQR92SMLzpRSvyTgpxyUt0anl0DeEwqQ
1xywOjDcYo2wDcGh9KHimFu4+ABi+xd3XHo/a0bjG2LAdluMMrr8+0SPzhqQRBz7d9p4icqOnjcG
TGMTKwL/MprFRWtowzo59Vb+BkQZLr6qhQwUy6e7HU5rf8S7ng1b9CE5b/Y/1GytRuZzrIGSSQep
F3a9u3UuJFf6TkiZ/F/DQUgGSNPoo/Hek50CAwEAAaOB2TCB1jAdBgNVHQ4EFgQUM/JziGyZzQAP
Thvn2bvneMGd3Z8wgaYGA1UdIwSBnjCBm4AUM/JziGyZzQAPThvn2bvneMGd3Z+heKR2MHQxCzAJ
BgNVBAYTAkVFMREwDwYDVQQIEwhNeSBTdGF0ZTEQMA4GA1UEBxMHbXkgQ2l0eTEVMBMGA1UECh
MM
Q29tcGFueSBOYW1lMRAwDgYDVQQLEwc3NzExMjIzMRcwFQYDVQQDEw53d3cubXlzaXRlLmNvbYIJ
AKcoY+m8gQgZMAwGA1UdEwQFMAMBAf8wDQYJKoZIhvcNAQELBQADggEBAA7Afh9bQGMrAbmWMzV
d
Sl0mipz7EdNvdHoB8uJ+/VN7+cPCl5Wv3gnBNxbK7pCKoH2ECnAD4o91RT9winoCLaduMCBWIdbV
5AiZbmPSOw52byIZn0MCTPW0dkphQtJdDRxtFFLzZQPLfUBF5xasSveF/JT09p/ukcbkmE6w7TPd
4ivHis0vPJAEooA4oVGBIEJHOkdThu0myX+VsDU1K2JCWQ2IkymJdkxgMOGEUFAHTd8Xo7Z5Guqv
WRA7YrvsR1tclN0FKS0ICbbuUb3nFxx2BboPvGC4H5dUagoVDrmotSChNVUVOLlE+YTI9ojyqMFB
pAhfSIiDh2jcOvPq1F4=
```

```
            </ds:X509Certificate>
          </ds:X509Data>
        </ds:KeyInfo>
      </ds:Signature>
    </ModirumMPI>
  </env:Body>
</env:Envelope>
```


PARes validation response from MPI:

```
<?xml version="1.0" encoding="utf-8" standalone="no"?>
<env:Envelope xmlns:env="http://www.w3.org/2003/05/soap-envelope">
  <env:Header/>
  <env:Body>
    <ModirumMPI xmlns="http://www.modirum.com/schemas/mpiapi"
xmlns:ns2="http://www.w3.org/2000/09/xmldsig#">
      <Message md="535CF439C39D63F978C1B58845C2005D" merchantId="sys1331720664552"
messageId="M1494972873437" version="4.0">
        <Response>
          <Parameters>
            <xid>VGnMqa+1jNBTSnCnoh3K8PuiVZQ=</xid>
            <mdStatus>1</mdStatus>
            <mdErrorMsg>Authenticated</mdErrorMsg>
            <enrollmenStatus>Y</enrollmenStatus>
            <authenticationStatus>Y</authenticationStatus>
            <eci>05</eci>
            <cavv>AAABAGI1kQAAAAAjcTWRAAAAAAA=</cavv>
            <cavvAlgorithm>2</cavvAlgorithm>
            <PAResVerified>true</PAResVerified>
            <PAResSyntaxOK>true</PAResSyntaxOK>
            <txId>13503</txId>
          </Parameters>
        </Response>
      </Message>
      <ds:Signature xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
        <ds:SignedInfo>
          <ds:CanonicalizationMethod Algorithm="http://www.w3.org/TR/2001/REC-xml-c14n-20010315"/>
          <ds:SignatureMethod Algorithm="http://www.w3.org/2001/04/xmldsig-more#rsa-sha256"/>
          <ds:Reference URI="#M1494972873437">
            <ds:DigestMethod Algorithm="http://www.w3.org/2001/04/xmlenc#sha256"/>
```

Copyright © 2006-2017 Modirum Ltd, 2017-2018 by VPOS Ltd.
The document may not be published or disclosed to a third party without the written permission of VPOS Ltd.

```
            <ds:DigestValue>sYLd56IRpCQN4GdMOrJpGCOhbAzP90u+Ew/8f/kPuf4=</ds:DigestValue>
          </ds:Reference>
        </ds:SignedInfo>
        <ds:SignatureValue>
qtFKBS+MrOeL1DKyOg8LYkM260DC4UViXutKKFhKto3A7kKfE0Ww1Zh+Ri4NNzehsDgi59NAINMD
EEQGh2Mlpjvjl35PO1GylLRyOOZMxsUjIFlxwDb/nHlNuQWPPADwBbtmQz7wHG60Boc9l5Z6IBI2
zGEtas6ZxPcbD8VLeOgZYg34TvjIY5K9giFyEdUYUyKw2HHaABXrjlndCFTr/3NeenqRAuI/vThh
uZyNLw99baE1qIZcMeHcq4CaBNM8EG4dgKETtda96PBUy/E6ykBp+VZooSwRm6Ts8JuRQVjPwH2S
BbxWIXwp15qSlw0wRwSCQugRBz2UC/REk/dVkA==
        </ds:SignatureValue>
        <ds:KeyInfo>
          <ds:X509Data>
            <ds:X509Certificate>
MIIEDDCCAvSgAwIBAgIJAPmMWIp6hdlRMA0GCSqGSIb3DQEBCwUAMGExCzAJBgNVBAYTAkVFMQ4w
DAYDVQQIEwVTVEFURTERMA8GA1UEBxMIbG9jYXRpb24xDDAKBgNVBAoTA29yZzELMAkGA1UECxMC
T1UxFDASBgNVBAMTC3d3dy5tcGkuY29tMB4XDTE3MDQxMDE0Mjk1NFoXDTIxMDQwOTE0Mjk1NFow
YTELMAkGA1UEBhMCRUUxDjAMBgNVBAgTBVNUQVRFMREwDwYDVQQHEwhsb2NhdGlvbjEMMAoGA1UE
ChMDb3JnMQswCQYDVQQLEwJPVTEUMBIGA1UEAxMLd3d3Lm1waS5jb20wggEiMA0GCSqGSIb3DQEB
AQUAA4IBDwAwggEKAoIBAQDABIBYhYb1eG3hNhmqaF6+TKd7FVnZZhRKZsRk4gOThpmQgb4JDc3G
o25m1RriU7K/ChRJG10FYfTWVdzhzFUPUljgkTK3Kw3/cxMGJVyBgB+E7MORYN83kZng0nSof+XB
di7jI37GjdY6YbQ2XhvOLHJVHuwVwMXa1oBtoFbH/xrIbZbADWXu/HSbaR646EKaatUZxrHGn+yS
b5cvzkVPJZWftMOv0vZSuJNmuWLjZ1fcibrY6k1Y8IyTBajTrrOv+logS3mNlVsSxRc/923O1Mqc
UlvGwMiTrsc/SFom1jkpkRmj3Tbf2xH+uGPI2sNJ0Y1oKGpjc2e92OGPcBNJAgMBAAGjgcYwgcMw
HQYDVR0OBBYEFKUAYaOMNxyv021FrFM/tQn67CzPMIGTBgNVHSMEgYswgYiAFKUAYaOMNxyv021F
rFM/tQn67CzPoWWkYzBhMQswCQYDVQQGEwJFRTEOMAwGA1UECBMFU1RBVEUxETAPBgNVBAcTCGxv
Y2F0aW9uMQwwCgYDVQQKEwNvcmcxCzAJBgNVBAsTAk9VMRQwEgYDVQQDEwt3d3cubXBpLmNvbYIJ
APmMWIp6hdlRMAwGA1UdEwQFMAMBAf8wDQYJKoZIhvcNAQELBQADggEBAGjOX36cEik4FDRuyIy9
gMzz36s8EPhEWd+b1RFJEvheOJOgnbrBZbd4OLrzW1JBzZ3qq1XRsFr+tw9zKCIpl6sVxgzKYt4O
Z2LKG1+N1OD9wHE9jZ1dYaRNEsmcurcyX6cRyIvNsT0ioJxNFSMGf5iJGYP+b88Ist5r1xs3rq8V
a2PLQ1rB4S02/U2C6h+iYWyYv95d9+acrwbPpIwvEFRWPUnR2gzgBL/Gs0O0jiNcNyuUR5nJDIUf
Us0ERAYWdRmRlEK7pmxqkhRqsLF2exWpmkK8rBGh5JD8908Nu9aB+efMDB4582J5vcz7VV2zwRKY
orvXz6ca1a62exlyoQw=
            </ds:X509Certificate>
          </ds:X509Data>
        </ds:KeyInfo>
      </ds:Signature>
    </ModirumMPI>
  </env:Body>
</env:Envelope>
```


Copyright © 2006-2017 Modirum Ltd, 2017-2018 by VPOS Ltd.
The document may not be published or disclosed to a third party without the written permission of VPOS Ltd.